Santa Clara University School of Law

Santa Clara High Technology Law Journal

Volume 20 | Issue 4 Article 2

2004

Spam After Can-Spam: How Inconsistent Thinking Has Made a Hash out of Unsolicted Commercial E-Mail Policy

Jeffrey D. Sullivan

Michael B. de Leeuw

SPAM AFTER CAN-SPAM: HOW INCONSISTENT THINKING HAS MADE A HASH OUT OF UNSOLICITED COMMERCIAL E-MAIL POLICY

Jeffrey D. Sullivan and Michael B. de Leeuw†

INTRODUCTION

The authors of the Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003 (hereinafter, "CAN-SPAM" or the "Act"),[1] the first United States federal law placing restrictions on the use of unsolicited commercial e-mail ("UCE"), or "spam," were asking for trouble. First, the title of the Act rings of Orwellian doublespeak. Second, its content has drawn ire from all sides except, for the most part, the direct marketers who are the ones being regulated – and that is not a good sign.

Despite the considerable fanfare that accompanied the Act's passage, including high profile lawsuits by Internet Service Providers ("ISPs") against unnamed John Doe spammers,[2] the reactions of both anti-spam activists, and of spammers, to the new law suggest that the Act has not had – and will not have – much effect in stemming the rising tide of spam that is clogging e-mailboxes the world over.

Some of the apparent weaknesses of CAN-SPAM as an effective tool to thwart spam arise from dubious drafting decisions, while others reflect the endemic shortcomings of any attempts to control spam by national legislation, given the inherent fluidity and anonymity of e-mail distribution through the Internet. In addition, long delay in enacting legislation – even flawed legislation – may

---

† Jeffrey D. Sullivan (jsullivan@bakerbotts.com) is an associate in the intellectual property group of the New York office of Baker Botts, L.L.P. He received his law degree from the University of Texas at Austin, where he was an associate editor of the Texas Law Review. Michael B. de Leeuw (deleemi@ffhsj.com) is an associate in the litigation department of the New York office of Fried, Frank, Harris, Shriver & Jacobson LLP. He received his law degree from Rutgers University (Newark), where he was editor-in-chief of the Rutgers Computer and Technology Law Journal.

1. Passed as Senate Bill S. 877, 108th Cong. (2003) (codified at 15 U.S.C. §§ 7701–7713, 18 U.S.C. § 1037).

2. *See infra* note 162.

well be responsible in part for the enormous explosion of spam that has made its control all the more difficult.

Spam is a serious problem on many fronts, but a more sophisticated analysis of spam and its related phenomena, than that performed by the authors of the Act, is necessary. Solving the spam problem requires undertaking philosophical, historical, technological, and economic analyses of the market forces that are at play. Only after considering the dynamic interplay of these factors will it likely prove possible to arrive at an effective solution to the spam problem.

I. THE ACT

Although Congress had been considering different anti-spam measures for many years,[3] it was slow to pass a legislative response to spam.[4] But in the face of an overwhelming public perception that spam was proliferating at an unacceptable rate,[5] recognizing that spam was imposing massive cumulative costs on American business and consumers,[6] and noting the inconsistent, and often stringent, state laws regulating spam, Congress finally acted in late 2003 to create a national standard for the acceptable use of e-mail solicitations.[7]

The Act recited a compelling list of Congressional Findings. Among these were:

---

3. Congress had been considering such measures since 1997. *See infra* notes 39–49.

4. The European Union, for instance, had finalized a Directive on Privacy and Electronic Communications ("DPEC"), providing, among other things, regulation of e-mail solicitations, by July 12, 2002. *See* DPEC, *at* http://www.dti.gov.uk/industries/ecommunications/directive_on_privacy_electronic_communications_200258ec.html.

5. *See* Enrique Salem, *Can-Spam Act is a Start*, CNET NEWS (Dec. 11, 2003), *at* http://news.com.com/2010-1028-5119513.html (noting public dissatisfaction with spam, then estimated to make up as much as 67% of all e-mail traffic).

6. *See, e.g.*, Jay Lyman, *Spam Costs $20 Billion Each Year in Lost Productivity*, E-COMMERCE TIMES (Dec. 29, 2003), *at* http://www.ecommercetimes.com/perl/story/32478.html (citing analysts' assertion that businesses' cost of dealing with spam were increasing at approximately 100% each year).

7. The CAN-SPAM Act is drawn by its terms not to "spam," but to "multiple commercial electronic mail messages" (with "multiple" being defined in specific numeric terms of messages sent per day, week, or month), a category that would presumably include, but not necessarily be limited to, UCE/spam. *See* S. 877, *supra* note 1 at § 4(d)(3). However, the Act does expressly exempt from the definition of the class of regulated/proscribed communications any "transactional or relationship messages," which are generally defined as communications from a business to its pre-existing customers with respect to a prior business transaction or ongoing business relationship. Messages from existing transaction partners have generally not been viewed as "spam" *per se* (because affirmative consent to receipt of such messages is inferred from the context of the prior transaction or ongoing business relationship). *Id.* § 3(17).

(1) The rapid growth in the volume of UCE threatened the convenience and efficiency of e-mail;[8]
(2) UCEs accounted for more than half of all e-mail traffic;[9]
(3) Most UCEs were fraudulent or deceptive;[10]
(4) UCE resulted in costs to recipients of UCE, including the costs of storage and costs associated with the time spent accessing, reviewing, and discarding the mail;[11]
(5) UCE was costly to ISPs, businesses, and educational institutions because of the need to increase storage or bandwidth or both;[12]
(6) The receipt of a large volume of UCE increased the chances that wanted e-mail would be discarded or ignored.[13]
(7) Many states had enacted mutually-inconsistent versions of anti-spam legislation that had not alleviated the spam problem and were difficult to enforce.[14]

CAN-SPAM attempted to address these identified problems in two ways: (1) by requiring that all commercial e-mail promulgators operate on an "opt out" basis, *i.e.*, they must provide recipients of a commercial message with a reliable means to elect not to receive any future mailings from the particular sender; and (2) by restricting certain common and deceptive practices employed by spammers, so as to provide greater transparency and accountability for senders of commercial e-mail.

The "opt out" provisions of CAN-SPAM are provided in Section 5(a) of the Act. These provisions make it a criminal offense to omit from any commercial e-mail a functional means of unsubscribing from future e-mails. All UCEs are to include advice to the recipient making it clear that the e-mail is of a commercial nature and that the recipient is entitled to opt out of future communications from the sender. Senders are also required to provide within any unsolicited commercial e-mail an accurate return postal address.[15]

8. S. 877, *supra* note 1 at § 2(a)(2).
9. *Id.*
10. *Id.*
11. *Id.* § 2(a)(3).
12. *Id.* § 2(a)(6).
13. *Id.* § 2(a)(4).
14. S. 877, *supra* note 1 at § 2(a)(11).
15. *Id.* § 5(a)(5)(iii).

The provisions aimed at stopping common deceptive spammer tactics include prohibitions against: use of forged e-mail headers and/or return addresses;[16] use of false or misleading subject lines;[17] "harvesting" of e-mail addresses by automated means;[18] hijacking of intermediate "relay" computers to disguise the origin of commercial e-mail;[19] continuing to send commercial e-mails to, or distributing to other spammers the e-mail addresses of, recipients who have opted out; and[20] use of multiple e-mail accounts for the purpose of concealing spam activities.[21] Additional provisions of the Act place further restrictions on sexually-oriented commercial e-mail.[22]

The CAN-SPAM Act also requires the Federal Trade Commission ("FTC"), the agency generally charged with enforcement of the Act,[23] to formulate and present to Congress plans for implementation of a "do not e-mail" list (modeled after the highly popular "do not call" lists recently implemented in the U.S. to curb telemarketing) by which consumers could globally opt out of all UCE, and a plan for electronic submission to the FTC, and handling of, consumer complaints regarding UCE.[24]

Violators of the CAN-SPAM Act could, based on the Act's enforcement provisions, incur serious civil and criminal penalties. A party who, for instance, was found to have forged e-mail headers, or to have hijacked relay computers to distribute spam, could (if other aggravating factors were found, such as that the spammer's activities were employed in aid of a separate fraudulent scheme) face up to five years imprisonment, in addition to fines and forfeitures.[25] In addition to initiating procedures under the specific provisions of the CAN-SPAM Act, the FTC is empowered to seek remedies against violators of the Act under its general consumer protection mandate and its

16. *Id.* §§ 4(a)(1), 3(8), 5(a)(1).

17. *Id.* § 5(a)(2).

18. *Id.* §§ 5(b)(1), 4(b).

19. *Id.* §§ 4(a)(1), 5(b)(1).

20. S. 877, *supra* note 1 at § 5(a)(4).

21. *Id.* §§ 4(a)(1), 5(b)(2).

22. *Id.* § 5(d) (requiring that any commercial e-mails regarding sexually-oriented materials, unless sent pursuant to the recipient's prior consent to receive such material, be clearly labeled as pertaining to adult subject matter and that the initially-viewable content of the e-mail not contain the sexually-oriented content).

23. *Id.* §§ 7(a), 7(d).

24. *Id.* §§ 9, 10, 11, 14(e).

25. S. 877, *supra* note 1 at §§ 4(b)-(c).

delegated powers to prevent deceptive trade practices by employing the enforcement provisions of the Federal Trade Commission Act.[26]

The CAN-SPAM Act's prohibitions also extend to those who, even without committing any violative conduct under the Act, conspire to commit such conduct. The Act thus in principle invokes the broad federal anti-conspiracy policies and remedies against even attempted spam schemes.[27] Finally, the Act provides that certain especially-egregious spam activity (such as employing automated address harvesting or "dictionary attacks" to generate lists of recipient e-mail addresses, or employing proscribed spam activities in connection with other crimes such as fraud or identity theft) can justify imposition of enhanced penal sentences. Under the federal sentencing guidelines, these enhanced penalties can apply either to the unlawful spamming activity itself, or to another crime that the perpetrator facilitated by such spamming.[28]

In addition to the basic, and in theory quite strong, enforcement mechanisms entrusted to the FTC, the CAN-SPAM Act also authorizes civil causes of action to be brought against violators of the Act by: (a) state attorneys general or other agencies, who can, absent FTC objection, seek injunctive relief, statutory damages up to $2,000,000 (with the additional possibility of punitive damages in special cases), and attorney's fees, for violations of the Act adversely affecting their state's citizens; and (b) ISPs adversely affected by violations of the Act, who can seek similar injunctive and statutory damages remedies, up to a recovery of $1,000,000. Finally, the prohibitions and penalties of the Act extend not just to the actual sender of UCE, but also to any businesses retaining or working in concert with such sender.[29]

II. THE SHORT (YET PERHAPS TOO LONG) LEGISLATIVE HISTORY OF THE CAN-SPAM ACT

The first attempts to enact federal laws to curb spam date back to 1995 (long before the first Nigerian billionaire philanthropist had earned his first naira). The first important anti-spam bill, the Unsolicited Commercial Electronic Mail Choice Act of 1997, was

26. *Id.* §§ 7(a), 7(d).
27. *Id.* § 4(a).
28. *Id.* § 4(b).
29. *Id.* § 6.

introduced by Senators Murkowski and Torricelli in 1997.[30] That bill required that: (a) "Advertisement" or "ADV" appear as the first word in the subject line of an e-mail;[31] (b) all routing information be accurate; [32] and (c) the UCE contain an opt-out provision.[33] The bill also would have allowed for FTC enforcement,[34] permitted actions to be brought by the states[35] or by individuals,[36] refrained from pre-empting state law,[37] and created a limited "opt-in" system. The "opt-in" system would allow customers to choose to receive UCE from particular sources even if the UCE did not comply with the other provisions of the Act, *e.g.*, such an e-mail would not need to contain "Advertisement" or "ADV" in the subject line.

The bill was fairly sophisticated, especially given the time when it was written, which was a relatively spam-free era. Its most important measure for controlling spam was the labeling requirement. This would have allowed an ISP or end user to filter out automatically e-mails that had "Advertisement" or "ADV" in the subject line. While this measure would only have worked if spammers complied with the law, given the relatively small volume of spam in 1997, it might well have curtailed the exponential growth of UCE. It certainly would have separated the legitimate, *i.e.*, complying, spammers from the illegitimate spammers, and effective enforcement might have even been possible against the non-complying spammers. The bill, however, was not acted on by Congress.[38]

---

30. Unsolicited Commercial Electronic Mail Choice Act of 1997, S. 771, 105th Cong. (1997), *available at* http://www.techlawjournal.com/congress/slamspam/s771is.htm.

31. *Id.* § 3.

32. *Id.*

33. *Id.* § 7(a)(1).

34. *Id.* § 4.

35. *Id.* §§ 5, 9.

36. *Id.* § 8.

37. *Id.* §§ 5, 9.

38. Another early congressional attempt to legislate spam was the Netizens Protection Act of 1997, H.R. 1748, 105th Cong. (1997). This proposal would have amended the Communications Act of 1934 to make it unlawful "to use any computer or other electronic device to send an unsolicited advertisement to an electronic mail address of an individual with whom such person lacks a preexisting and ongoing business or personal relationship, unless such individual provides express invitation or permission."

The original version of the CAN-SPAM Act[39] was introduced along with nine other anti-spam bills during the 106th Congress (1999-2000).[40] The original bill included many of the features that were ultimately passed into law, including the criminal sanctions, the opt-out approach, and the general enforcement powers given to the FTC.[41] None of these early bills was signed into law, and, indeed, none was even close to getting out of Congress until 2003.[42]

There is little explanation for why Congress did not act for so long while the problem of spam got steadily worse. While there was considerable lobbying by direct marketing associations, the main issues that concerned them were the use of "Advertisement" or "ADV" labeling in headers, the possibility of an "opt-in" provision, and the possibility of a private cause of action. Marketers were, of course, vehemently opposed to such provisions. While there was never a serious "opt-in" bill proposed in Congress, there were, as noted, several bills that had labeling provisions. The direct marketers strongly opposed labeling provisions publicly, citing First Amendment reasons.[43] Perhaps a more cogent reason for their

39. The first bill entitled "Can Spam" was introduced in the House of Representatives by Congressman Gary Miller. *See* Can Spam Act, HR 2162, 106th Cong. (1999), *available at* http://www.techlawjournal.com/cong106/spam/hr2162ih.htm. Except for the name, however, there is little connection between this act and the one that was passed in 2003. In 2000, Senators Burns and Wyden, the authors of the ultimately enacted CAN-SPAM Act introduced the first version of their bill, Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2000. S. 2542, 106th Cong. (2000) [hereinafter "CAN SPAM I"].

40. The others were: the Inbox Privacy Act of 1999, S. 759, 106th Cong. (1999); the Unsolicited Electronic Mail Act of 2000, H.R. 3113, 106th Cong. (1999); the Internet Growth and Development Act, HR 1685, 106th Cong. (1999); the Internet Freedom Act, HR 1686, 106th Cong. (1999); the E-Mail User Protection Act, HR 1910, 106th Cong. (1999); the E-Mail User Protection Act, H.R. 1910, 106th Cong. (2000); the Netizens Protection Act of 1999, H.R. 3024, 106th Cong. (1999); the Protection Against Scams on Seniors Act of 1999, H.R. 612, 106th Cong. (1999); and the Wireless Telephone Spam Protection Act, H.R. 5300, 106th Cong. (2000). Links for all of these bills are available at:
http://www.spamlaws.com/federal/summ106.html#hr3113.

41. CAN SPAM I, *supra* note 39.

42. Daniel Tynan, *Antispam Legislation Lags*, PC WORLD (Sept. 19, 2003), *available at* http://www.pcworld.com/news/article/0,aid,112554,00.asp (noting that the 107th Congress had considered eight anti-spam bills without acting on any of them).

43. *See, e.g.*, Declan McCullagh and Robert Zarate, *Spammers Slam Anti-Spam Proposals*, WIRED, Mar. 28, 2002, *available at* http://www.wired.com/news/politics/0,1283,51370,00.html?tw=wn_story_related (quoting the Direct Marketing Association's President, Jerry Cerasale, as saying, "Going to the First Amendment issue, the unsolicited commercial e-mail issue has been applied to non-profits trying to get funds. Courts have ruled that's protected as speech. . . . We look at ADV as labeling speech and we oppose that," and describing the American Civil Liberties Union and the Electronic Frontier Foundation as holding a similar view.).

opposition was the ease with which an e-mail could be filtered and discarded if it contained "ADV" in the header.

The 108th Congress ultimately passed the CAN-SPAM Act, but not before introducing eight other bills.[44] The striking thing about the nine bills that were considered by the 108th Congress is how similar they were. Other than the Criminal Spam Act of 2003[45] and the Wireless Telephone Spam Protection Act[46] (both of which were specialized bills that dealt with only a particular technology), all of the anti-spam measures had some sort of "opt out" provision or "'no spam' registry" model for the control of spam.[47] And only two bills, the Stop Pornography and Abusive Marketing Act[48] and the Reduce Spam Act of 2003,[49] had labeling requirements, requiring spammers to identify spam with an "ADV" label in a header. No bills introduced included "opt-in" measures, and no other radical measures were thrown into the hopper such as, for example, a postage requirement for e-mail advertisements.

It is not surprising, therefore, that the final version of the CAN-SPAM Act, which was passed by the Senate on November 25, 2003, agreed to by the House of Representatives on December 8, 2003, and signed by the President on December 16, 2003, was very similar to the first version of the bill, introduced in 1999. It was also very similar to most of the other bills under consideration. This raises the question, why was nothing done about spam while the volume of spam spiraled out of control between 1997 and 2004?

Obviously, Congress and the nation had other important matters to consider during this period, and the ever-increasing number of "penis enlargement" e-mails was just an increasing nuisance for most. However, it is interesting to question whether the long delay in passing comprehensive legislation has itself contributed to exponential increase in spam. It is possible that, had a comprehensive

---

44. They were: the Anti-Spam Act of 2003, H.R. 2515, 108th Cong. (2003); the Ban on Deceptive Unsolicited Bulk Electronic Mail Act of 2003, S. 1052 (108th Cong. (2003); The Computer Owners' Bill of Rights, S. 563, 108th Cong. (2003); the Criminal Spam Act of 2003, S. 1293, 108th Cong. (2003); the Reduce Spam Act of 2003, H.R. 1933, 108th Cong. (2003); the Reduction in Distribution of Spam Act of 2003, H.R. 2214, 108th Cong. (2003); the Stop Pornography and Abusive Marketing Act, S. 1231, 108th Cong. (2003); and the Wireless Telephone Spam Protection Act, H.R. 122, 108th Cong. (2003). *See* http://www.spamlaws.com/federal/summ108.html#hr2515.

45. S. 1293, 108th Cong. (2003).

46. H.R. 122, 108th Cong. (2003).

47. *See* http://www.spamlaws.com/federal/summ108.html#hr2515.

48. S. 1231, 108th Cong. (2003).

49. H.R. 1933, 108th Cong. (2003).

anti-spam law had been enacted in the late 1990s, even one with the problems inherent in the CAN-SPAM Act, spam would never have spiraled out of control. The lack of any federal law allowed spammers to become increasingly rich and savvy. They were able to analyze the approaches that Congress was considering, and in the case of legitimate marketers, they had the time to influence (if not suborn) the legislative process through lobbying.

III. ALL BARK, NO BITE?

Based on the considerable fanfare that accompanied its passage and its facially-impressive enforcement provisions, the CAN-SPAM Act might be expected to provide hope to beleaguered spam recipients and to engender fear (and compliance) on the part of bulk commercial e-mailers. So far, however, neither of these outcomes has been evident.[50]

Anti-spam activists and other commentators have, to the contrary, blasted the CAN-SPAM Act as intrinsically flawed and compromised from the start. Probably the biggest policy-based complaints from the anti-spam camp are that the Act shifts the burden of avoiding unsolicited e-mail, in the first instance, from the sender to the receiver, by virtue of its "opt out" provisions.[51] Vocal anti-spam advocates have derisively dubbed the Act the "You-Can-Spam" Act, arguing that it provides a federal imprimatur for unsolicited e-mail by deeming it presumptively lawful as long as accurate return address/header information, and functional "unsubscribe links" are

50. *See, e.g.*, Lee Rainie and Deborah Fallows, *The CAN-SPAM Act Has Not Helped Most Email Users So Far: Disillusionment is Growing as 29% of Email Users Say They Are Using Email Less Because of Spam*, Pew Internet Project Data Memo, Mar. 2004 ("March 2004 Pew Study"), *available at* http://www.pewinternet.org/reports/pdfs/PIP_Data_Memo_on_Spam.pdf (describing Pew Internet survey that shows that CAN-SPAM has been generally ineffective); Andy Sullivan & Eric Auchard, *Progress in War Against Spam Hit or Miss*, Reuters (Apr. 11, 2004), *at* http://www.reuters.com/newsArticle.jhtml?storyID=4798222 (quoting market researchers' estimates that "the worldwide spam epidemic is expected to jump to 35 billion messages from 15 billion in 2003" and noting that "most surveys show that volume has not dropped since the U.S. [CAN-SPAM] law took effect in January.").

51. *See, e.g.*, Spamhaus Position on CAN-SPAM Act of 2003 (S. 877/H.R. 2214), *at* http://www.spamhaus.org/position/CAN-SPAM_Act_2003.html ("Spamhaus sees the introduction of the CAN-SPAM Act of 2003 (S.877/HR 2214) as a serious failure of the United States government to understand the Spam problem."). *See also* Grant Gross, *CAN-SPAM Law: Little Impact So Far*, INFOWORLD (May 20, 2004), *at* http://www.infoworld.com/article/04/05/20/HNcanspamimpact_1.html.

provided.[52] E-mail users are justifiably wary of unsubscribe links. Such links have become fatally tainted because of spammers' employment of bogus links, or worse, links that actually serve to verify the recipient's e-mail address as a prime target for further spam.[53] Therefore, it is not clear that consumers will be willing to rely upon purported unsubscribe links even when they are legitimate, functional, and in compliance with CAN-SPAM. Critics also point out that the Act pointedly refrains from providing any private right of action to individual victims of spam. Instead, it vests all enforcement authority in the hands of federal and state agencies and, to some extent, ISPs.[54]

---

52. *See, e.g., United States set to Legalize Spamming on January 1, 2004*, SPAMHAUS, *at* http://www.spamhaus.org/news.lasso (providing commentary from leading anti-spam website spamhaus.org):

> Against the advice of all anti-spam organizations, the U.S. House of Representatives has passed the CAN-SPAM Act, a bill backed overwhelmingly by spammers and dubbed the "YOU-CAN-SPAM" Act because it legalizes spamming instead of banning it. Spam King Alan Ralsky told reporters the passage of the House bill "made my day." Spammers say they will now pour money into installations of new spam servers to heavily ramp up their outgoing spam volumes "all legally."
>
> . . .
>
> With the passage of CAN-SPAM, spamming will be officially legal throughout the United States, CAN-SPAM says that 23 million U.S. businesses can all begin spamming all U.S. email addresses as long as they give users a way to opt-out, which users can do by following the instructions of each spammer. Anyone with any sense would of course realize that if CAN-SPAM becomes law, opting out of spammers lists will very likely become the main daytime activity for most U.S. email users in 2004. The second main activity will be sorting through mailboxes crammed with 'legal' spam every few minutes to see if there's any email amongst the spam.

53. *See, e.g.*, Hermit, *National SPAM Law Not as Bad as Utah's*, UTAH POLITICS (Dec. 16, 2003), *at* http://www.utahpolitics.org/archives/oooo19.shtml ("[C]ompetent computer professionals will tell you to never hit unsubscribe, as it verifies your address.").

54. *See, e.g., CAN-SPAM May Help Curtail Spam, but Bill Has Some Troubling Provisions*, CDT POLICY POST, Volume 9, Number 23 (Dec. 12, 2003), *available at* http://www.cdt.org/publications/pp_9.23.shtml ("[T]he CAN-SPAM Act lacks what might have been the most effective means of enforcement – a narrowly drawn individual right of action."). Laws restricting unsolicited commercial communications in other contexts have provided private rights of action (*cf.* 47 U.S.C. § 227, the "anti junk fax" law, permitting recipients of unsolicited advertising facsimiles to seek damages of up to USD$1,500 in small claims court) have been regarded as highly successful deterrents to abusive solicitations, by creating hundreds of "private attorneys general" to pursue miscreants whose activities might otherwise escape pursuit by the government's investigative apparatus. *See* Lori Enos, *Can Spam Ever Be Stopped?*, E-COMMERCE TIMES (May 14, 2001), *at* http://www.ecommercetimes.com/perl/story/9581.html (quoting expert to the effect that "most fax spammers 'stopped pretty quickly' after the junk-fax law was passed" due in part to its private right of action provision).

Anti-spam activists further view with great suspicion the fact that the CAN-SPAM Act enjoyed enthusiastic support from many direct marketers and other users of UCE, who feared, but managed through their lobbying to avert, more stringent and, as the activists assert, more effective, legislation.[55] In particular, the direct marketers were successful at ensuring that the federal law that was approved by Congress and signed into law did not contain a labeling requirement that would require all UCE to include "ADV" (or some variant) in headers. Such a requirement would have made technological spam solutions easier by allowing ISPs or end users to be able to filter legally-compliant UCE with ease. Of course, this would have done nothing to deal with the issue of illegitimate UCE, *i.e.*, spam sent by spammers who were not complying with the law.

Another factor that may add to the skepticism regarding the efficacy of CAN-SPAM is that even the penalties that it does make available are to be enforced in the first instance by the FTC, which brings to the fray of spam fighting a slate largely clean of any significant victories or effective action against spammers.[56] For instance, the FTC has long accepted consumers' e-mail submissions of deceptive UCE. Rather than taking any action on individual fraudulent spam communications, though, the FTC has simply "archived" the spam in an impressively-comprehensive, but not obviously useful, "museum of spam."[57] The FTC's chairman has voiced his opposition to a "do not e-mail list" and expressed his belief that "legislation cannot do much to solve the spam problem." Some industry observers have voiced similarly-pessimistic views about the true feasibility of enforcing compliance on rogue spammers who hide

---

55. *See, e.g.*, David Berlind, *Score one for the spammers: CAN SPAM bill to become law*, TECH UPDATE (Nov. 30, 2003), *at* http://techupdate.zdnet.com/techupdate/stories/main/Score_one_for_the_spammers.html ("It's no wonder the [Direct Marketing Alliance, a coalition of bulk advertisers] likes the CAN SPAM bill. It gives marketers unbridled rights to invade our inboxes at least once."); *see also* Joseph J. Lewczak and Ivana Starr, *Congressional Cure-All For Consumers' Clogged Inboxes: Federal Law Provides Uniform Set of Commercial Email Rules*, FINDLAW.COM, *at* http://articles.corporate.findlaw.com/articles/ file/01009/009360 (providing summary of the Act by counsel for e-mail marketing companies: "The Act's impact on state SPAM laws is a tremendous victory for the marketing industry.").

56. *See, e.g.*, Stephen H. Wildstrom, *Why Spammers Laugh at CAN-SPAM*, BUSINESSWEEK ONLINE (Jan. 7, 2004), *at* http://www.businessweek.com/technology/content/jan2004/tc2004017_2996_tc078.htm ("But neither the overburdened FTC nor hard-pressed U.S. Attorneys get any new enforcement resources [to enforce the CAN-SPAM provisions].").

57. *See* Michelle Delio, *FTC: Where Spam Goes to Die*, WIRED (Nov. 5, 2002), *available at* http://www.wired.com/news/politics/0,1283,55972,00.html (quoting FTC staff attorney: "No one sits down and actually reads all the spam that we receive daily. . . . That would be incredibly boring and totally futile.").

behind the Internet's anonymity. Still, such sentiments appear in dubious, defeatist taste coming from the head of the agency charged with attempting to make such legislation effective.[58] The supine FTC also has not shown itself especially imaginative in applying prior laws to thwart spam – it has not, for instance, taken the aggressive, but not unjustifiable, position that sending UCE with forged headers and return/unsubscribe information is by itself (regardless of the UCE's other content) an instance of wire fraud under 18 U.S.C. § 1843.[59]

IV. IS CAN-SPAM THE RUNT OF THE SPAM-FIGHTING LITTER?

Beyond its dubious pedigree, the Act suffers, in the eyes of some, by comparison with enacted and proposed anti-spam legislation or regulations from other jurisdictions, at least some of which were viewed by anti-spam organizations as having considerably more potential to cut down on spam. Many states had enacted laws that dealt, or would have dealt, with spam in a number of effective ways.[60] Other countries have also enacted UCE-related laws that span the gamut of spam control approaches.

A. Alternate (And Now-Mooted) State Approaches

In all, 38 states enacted some form of law that reached spam and spamming activities. The CAN-SPAM Act explicitly pre-empts most state laws concerning UCE, including the far more stringent laws that were already on the books in California and elsewhere.[61] At least

58. *See FTC Chairman Calls Spam "One of the Most Daunting Consumer Protection Problems FTC Has Ever Faced,"* FEDERAL TRADE COMMISSION (Aug. 19, 2003), *available at* http://www.ftc.gov/opa/2003/08/aspenspeech.htm#36237.

59. The elements of wire fraud under Section 1843 are: (1) that the defendant voluntarily and intentionally devised or participated in a scheme to defraud another out of money; (2) that the defendant did so with the intent to defraud; (3) that it was reasonably foreseeable that interstate wire communications would be used; and (4) that interstate wire communications were in fact used. In the UCE context, the FTC might have argued that that recipients of forged UCE, who may spend thousands of dollars maintaining their e-mail servers and implementing spam filters, are "defrauded" of this investment to the extent that they rely upon the spammer's false representation that its message is a legitimate commercial communication, that unsubscribing from the UCE is possible, and that the source of the e-mail is the (forged) returned address; in essence, the spammer is shifting the cost of transmitting and displaying his advertising from himself to the receiving company's e-mail servers.

60. As noted, *supra*, these state laws are now pre-empted by the Act. An excellent source for information regarding state and international spam laws is Professor David Sorkin's spamlaws.com website. It contains links to all enacted (and some un-enacted) spam laws, both domestic and international. *See* http://www.spamlaws.com.

61. *See* S. 877, *supra* note 1 at § 8(b); *see also* Joseph J. Lewczak and Alison DeGregorio, *California's New SPAM Law Has Been Pre-empted by the Passage of the Federal CAN SPAM Act of 22003, Which Goes into Effect on January 1, 2004*, FINDLAW.COM, *at*

some of these state laws contained (or, if allowed to come into force, would have contained) proscriptions and penalties viewed by anti-spam forces as more effective, and as properly placing more of the burden of spam avoidance squarely on marketers, not e-mail recipients.

1. Opt-In Approaches

California and Delaware were pioneers in anti-spam legislation. Both adopted an "opt-in" approach to spam,[62] making *all* UCE unlawful unless the recipient had previously indicated consent to its receipt.[63] The "opt in" rule is in contrast to CAN-SPAM's "opt out" provision, which makes at least the first unsolicited commercial e-mail sent to a recipient lawful so long as he can affirmatively opt out of future spam.

While the similarly-phrased Delaware "opt-in" law was a criminal statute only, the California "opt-in" law also would have

---

http://articles.corporate.findlaw.com/articles/file/01009/009210; *but see* Amit Asaravala, *Taking a Second Shot at Spammers*, WIRED NEWS (Apr. 23, 2004), *at* http://www.wired.com/news/politics/0,1283,63181,00.html (noting that the Act expressly reserves from pre-emption state laws regulating e-mail based upon the falsity or deception of its contents, and noting efforts by California officials to re-pass legislation compliant with the safe harbor); *see also* S. 877, *supra* note 1 at § 8(b)(1)–(2) (allowing for survival of state laws as applied to e-mail to the extent that "any such statute, regulation, or rule prohibits falsity or deception in any portion of a commercial electronic mail message or information attached thereto," as well as exempting from pre-emption "State laws that are not specific to electronic mail, including State trespass, contract, or tort law; or . . . other State laws to the extent that those laws relate to acts of fraud or computer crime.").

62. *See* CAL. BUS. & PROF. CODE § 17529.2 (2003) (superseded) (rendering it illegal to, *inter alia*, "(a) Initiate or advertise in an unsolicited commercial e-mail advertisement from California or advertise in an unsolicited commercial e-mail advertisement sent from California [or] (b) Initiate or advertise in an unsolicited commercial e-mail advertisement to a California electronic mail address, or advertise in an unsolicited commercial e-mail advertisement sent to a California electronic mail address," as well as to use common spammer techniques such as "spoofing" (or forging) return address headers or falsifying subject lines (§ 17529.5) or conducting automated address harvesting (§ 17529.4)); DEL. CODE TITLE 11 CRIMES AND CRIM. PROC. § 937 (making it a criminal offense for a person to intentionally or recklessly send a UCE unless there is prior consent or a prior business relationship between the parties).

63. CAL. BUS. & PROF. CODE § 17529.1 (defining "unsolicited commercial e-mail advertisement" as "a commercial e-mail advertisement sent to a recipient who meets both of the following criteria:

> (1) The recipient has not provided direct consent to receive advertisements from the advertiser.
>
> (2) The recipient does not have a preexisting or current business relationship, as defined in subdivision (l), with the advertiser promoting the lease, sale, rental, gift offer, or other disposition of any property, goods, services, or extension of credit").

provided a private right of action for spam recipients (unlike the CAN-SPAM regime in which civil enforcement authority is left to agencies and ISPs). The California law never went into effect as it was pre-empted before it became effective.

2. Labeling Approaches

Sixteen states had enacted legislation that required all UCE to include "ADV," "Advertisement" or a similar word in their e-mail headers.[64] As noted above, this approach was directly at odds with the lobbying efforts of the legitimate direct marketers, who feared the ease with which their messages could be filtered under such a regime.

Indeed, one of the likely reasons that the CAN-SPAM Act finally passed through Congress in 2003 is that the direct marketers, who in the absence of state laws would have presumably happily gone unregulated, were concerned about the more stringent state approaches, many of which (including California's very stringent law) were enacted in 2003. CAN-SPAM provided a clear two-fold victory for the direct marketers. It pre-empted more stringent state laws while eschewing the approaches that direct marketers most feared, i.e., the "opt-in" approach, the labeling approach, and the private cause of action approach.[65]

B. Approaches In Other Countries

Critics have likewise argued that CAN-SPAM's relatively marketer-friendly approach is at odds with anti-spam laws from other countries, especially those adopted by the European Union. The European Union finalized a Directive on Privacy and Electronic Communications ("DPEC"), providing, among other things, regulation of e-mail solicitations.[66] The DPEC took an "opt in" approach to most UCE. Countries such as the United Kingdom and Italy have now, pursuant to the DPEC, put into force regulations requiring prior opt-in before any commercial e-mail can be sent to an individual consumer, although the regulations permit an "opt out"

64. These states were: Arizona, Colorado, Illinois, Indiana, Kansas, Kentucky, Maine, Michigan, Minnesota, New Mexico, North Dakota, Oklahoma, Oregon, South Dakota, Tennessee, and Texas. *See* SPAMLAWS.COM, *at* http://www.spamlaws.com/state/summary.html.

65. This is not to mention the idea of requiring an e-mail stamp for either advertisements or for all e-mail, an idea that Bill Gates has recently discussed publicly. *See* John Hogan, *Will Gates' email Postage Idea Stamp Out Spam?*, Feb. 6, 2004, *available at* http://searchwin2000.techtarget.com/columnItem/0,294698,sid1_gci949091,00.html. Obviously such a provision, if enforceable, would disproportionately affect direct marketers.

66. DPEC, *supra* note 4.

approach as to UCE sent to businesses.[67] While it is too early to assess the efficacy of such laws, early results appear to be mixed.[68]

Other countries are adopting anti-spam legislation, but it is difficult to tell the effect that these laws are having or will have. One of the most facially impressive anti-spam laws is the new Australian Spam Act 2003,[69] which went into effect in April 2004. It is an "opt-in" law that also imposes additional significant restrictions on commercial e-mail that is lawfully sent.

C. Spam Litigation

In the pre-CAN-SPAM world, parties adversely affected by spam often resorted to litigation to redress their harm, often relying on common law doctrines such as trespass to chattels.[70] Several ISPs have received injunctive relief against spammers who have used their systems.[71] There are clear limitations to such actions, however, including the need to demonstrate actual injury.[72]

More fundamentally, a recurrent problem with litigation as a first-line remedy against spammers is that it is not easy to identify most spammers. The UCE senders whom one is likely to be able to identify with ease will most likely be the "legitimate" businesses whose UCE contains valid unsubscribe links and undisguised return addresses in its solicitations relating to legitimate goods and services. However, such "legitimate" UCE does not provoke the wrath of recipients, or pose all of the same problems, to the extent that

---

67. *See* DPEC, *supra* note 4; *see also* The Privacy and Electronic Communications (EC Directive) Regulations 2003, *available at* http://www.learnsteps4profit.com/antispamuk.html; John Leyden, *UK anti-spam law goes live,* THE REGISTER (Dec. 10, 2003), *at* http://www.theregister.co.uk/content/6/34443.html.

68. *See, e.g.*, John Leyden, *supra* note 67 (reporting sampling in early January, 2004 showing that only three of 1,000 UCE samples contained the CAN-SPAM-mandated information and links).

69. Spam Act, No. 129, 2003 (2003), *available at* http://scaleplus.law.gov.au/html/comact/11/6735/rtf/1292003.rtf.

70. *See generally* David E. Sorkin, *Technical and Legal Approaches to Unsolicited Electronic Mail*, 35 U.S.F. L. REV. 325 (2001). Professor Sorkin also maintains an excellent website that contains information and links to all things spam. *See* http://www.spamlaws.com/

71. *See, e.g.*, Compuserve, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Oh. 1997) (granting preliminary injunction in favor or an ISP against a spammer on a "trespass to chattels" theory); Hotmail v. Van$ Money Pie, 47 U.S.P.Q.2d (BNA) 1020 (N.D. Cal. Apr. 16, 1998) (granting preliminary injunction in favor of an ISP against a spammer on "trespass to chattels" theory, for Violations of the Computer Fraud And Abuse Act, 18 U.S.C. § 1030, and for other deceptive acts).

72. *See* Intel Corp. v. Hamidi, 30 Cal. 4th (2003) (holding that Intel could not prevail on a "trespass to chattels" theory when messages sent by a former Intel employee to current Intel employees that disparaged Intel did not damage the computer system or impair its function).

anonymous UCE, hawking bogus products and completely masking its sender's identity, does.

V. EARLY FRUITS OF CAN-SPAM: LESS THAN PROMISING

That the CAN-SPAM Act falls well short of successfully addressing the very problems that Congress correctly found were caused by rampant spam can hardly be doubted. Spammers themselves seem to have come to the conclusion that, Act or no Act, they may with impunity continue with business as usual. Indeed, early indications are that the vast majority of UCE continues not to comply with the Act's requirements regarding opt out capabilities, accurate signature and address information, and non-forged headers.[73]

By most accounts, the volume of spam has increased since the effective date of the Act.[74] Public irritation with spam appears to be reaching new heights, and willingness to wade through spam to enjoy the benefits of e-mail and the Internet may be sinking to new lows.[75] It is not even possible to say that the rate of increase of spam incidence (let alone its overall prevalence) has substantially slowed, given that most estimates for the overall proportion of e-mail that is spam (now ranging in the 50%-80% area)[76] were, as recently as only a year ago, in the comparatively modest range below 50%.[77]

---

73. *See* Leyden, *supra* note 67.

74. *See, e.g.*, Gregg Keizer, *CAN-SPAM Still Failing To Slow Junk Mail*, TECHWEB NEWS (Feb. 4, 2004) (noting that in the first month after the Act became effective, spam control firms had observed either no drop-off, or an increase, in the percentage of incoming mail that was made up by spam, with one filtering company reporting that an astonishing 79% of processed e-mail was spam); Lee Rainey & Deborah Fallows, *The impact of CAN-SPAM legislation*, PEW INTERNET & AMERICAN LIFE PROJECT (Mar. 2004), *at* http://www.pewinternet.org/reports/pdfs/PIP_Data_Memo_on_Spam.pdf (reporting that a greater proportion of e-mail users (24% and 19% of home and business e-mail users, respectively) had observed net increases in incoming spam from January through March 2004 than had observed any diminution (only 20% and 11% of users, respectively)).

75. *See* Rainey & Fallows, *supra* note 50 (reporting that 77% of e-mail users reported that spam made being online unpleasant and annoying, versus 70% expressing this sentiment in a similar survey in Summer, 2003).

76. *See, e.g.*, Press Release, *Spam levels will peak at 80 percent of all Internet email*, BRIGHTMAIL (Feb. 10, 2004), *at* http://www.brightmail.com/pressreleases/021004_apac-80-percent-spam.html ("[S]tatistics have shown spam levels hitting 60 percent of all email in January 2004, up from just 40 percent a year ago."); Allen Wastler, *Got more spam now?*, CNN.COM (Feb. 6, 2004), *at* http://money.cnn.com/2004/02/04/commentary/ wastler/wastler/ (citing incidence of spam as 60% of all e-mail ("a new high!") and arguing that CAN-SPAM may have exacerbated spam problem worldwide by emboldening U.S.-based spammers by virtue of its opt-out provisions, as opposed to European-style opt-in provisions).

77. *See, e.g.*, Press Release, *Earthlink Provides Consumer Advice For Fighting Spam*, EARTHLINK (Apr. 29, 2003), *at* http://www.earthlink.net/about/press/pr_consumerspamadvice/

Although private parties, such as ISPs, have started bringing civil litigation based on the CAN-SPAM Act,[78] governmental enforcement action has proceeded more slowly. The FTC has brought only one criminal prosecution under CAN-SPAM to date,[79] and no state attorney general appears to have initiated major criminal or civil proceedings under the Act to date. The FTC continues to conduct rulemaking proceedings to determine specific guidelines for enforcing CAN-SPAM. The rulemaking proceedings for the proposed do-not-e-mail list have been dominated by negative comments from marketing companies who oppose as impractical any limitations on their e-mail activities[80] (a viewpoint in line with the FTC chairman's expressed sentiments against a registry). Thus, the odds of the rulemaking process leading to a hard-line implementation of the Act seem chancy at best.

Federal sentencing guidelines for criminal violations of the Act issued from the United States Sentencing Commission in April. Commentators have characterized the provisions of the guidelines as "stiff,"[81] noting that they treat spam violations analogously to fraud and theft.[82] It remains to be seen how much zeal the agencies and prosecutors charged with implementing such stiff penalties will show, and whether they will be able to overcome the previously-prevalent mindset expressed by one criminal defense lawyer incensed by the

("Reports indicate that spam accounts for more than 40 percent of all email traffic on the internet.").

78. *See infra* Section VI(f).

79. *See* Ted Bridis, *U.S. charges four under new law against spam*, USA TODAY (Apr. 28, 2004), *at* http://www.usatoday.com/tech/news/2004-04-28-spam-charges-filed_x.htm (detailing charges against four Detroit-based UCE promulgators whose millions of solicitations had generated over ten thousand complaints to the FTC, and noting the indictment's assertion that the accused spammers had engaged in classic spam techniques, such as hijacking relay computers, to conceal the origin of their advertisements for dubious quasi-medical and personal enhancement products).

80. Tim Lemke, *Companies protest any do-not-spam list*, WASHINGTON TIMES (Apr. 12, 2004), *available at* http://washingtontimes.com/business/20040412-094511-7658r.htm ("Fifteen of the 17 public comments made available to reporters by the FTC argue against the registry. They include submissions from the Direct Marketing Association, Visa Inc., several e-mail publishers and a host of local real estate associations.").

81. *See, e.g.*, Paul Festa, *Stiff spam penalties urged*, CNET NEWS (Apr. 14, 2004), *at* http://news.com.com/2100-1028-5191651.html.

82. *See* News Release, *Sentencing Commission Toughens Requirements For Corporate Compliance And Ethics Programs*, UNITED STATES SENTENCING COMMISSION (Apr. 13, 2004), *at* http://www.ussc.gov/PRESS/rel0404.htm (noting that "[t]he Commission created a sentence enhancement of approximately 25 percent if a defendant improperly obtains e-mail addresses for the purpose of spamming and an automatic application of an additional 25 percent sentence increase for mass marketing. Additional sentencing increases based on the amount of loss and number of victims also will apply.").

extent of the criminal penalties now theoretically available under the Act: "'Congress made it a felony, but it's not the kind of misconduct that causes what we typically consider as harm to victims,' said Jack King, a representative for the National Association of Criminal Defense Lawyers. 'The whole idea behind the federal sentencing guidelines was to make the punishment fit the crime. But this is just junk mail. This doesn't even kill trees.'"[83] It is now up to the FTC and the states' attorneys general to show that they do not share this sanguine view.

To be fair, it is not completely clear that the inclusion of more stringent anti-spam terms in the CAN-SPAM Act, or more vigorous action by the FTC and other oversight agencies, would by itself have led to a substantial or immediate diminution in spam, as even jurisdictions that have adopted strict "opt in" rules are not necessarily going to see meaningful diminutions in the incidence of non-compliant solicitation e-mails.[84]

In fact, some have suggested that no legal approach can successfully stop spam. Their pessimism is founded upon the multi-jurisdiction problems of tracking and holding accountable anonymous spammers operating through computers and relays in multiple remote countries and the low barriers to entry allowing new spammers readily to spring up and replace any other spammers who might be identified and put out of business.[85] On this view, the only parties affected by or compliant with anti-spam legislation will be the good and accountable corporate citizens who would be likely, even absent such legislation, to honor their customers' preferences not to receive solicitations.

On the other hand, given that some authorities assert that the great majority of spam originates from just a handful of spam gangs,

---

83. Festa, *supra* note 81.

84. *See, e.g.*, John Leyden, *UK anti-spam law goes live,* THE REGISTER (Dec. 10, 2003), *available at* http://www.theregister.co.uk/content/6/34443.html (quoting U.K.-based spam expert: "Email users should not expect to see a huge impact on the volume of junk email they receive [following implementation of the U.K.'s opt in rules for e-mails to consumers]."); Motez Bishara, *New anti-spam laws fail to bite*, CNN.COM (Jan. 12, 2004), *at* http://www.cnn.com/2004/TECH/internet/01/12/spam.continues/index.html (quoting compliance manager for Information Commissioner's Office, the body responsible for enforcing U.K.'s partial-opt-in spam regulation: "'We don't have the swift injunctive powers that we need to act against those abusing the medium. A lot of people assume the law is stronger than it is.'").

85. *See, e.g.*, Anita Ramasastry, *Why the New Federal "CAN Spam" Law Probably Won't Work*, FINDLAW.COM (Dec. 3, 2003), *at* http://writ.corporate.findlaw.com/ramasastry/20031203.html ("Ultimately, the real solution to spam, I believe, will be more likely technological than legal, or some combination of these two, and potential other, approaches.").

many based in the U.S. or other identifiable locations,[86] it seems inadvisable to despair entirely of a judicial and law enforcement approach that could hope to put a significant dent in spam simply by locking up or bankrupting the spam kingpins. At the same time, the computer and e-mail industry will be pursuing more and more potent technological measures (such as Bayesian filtering and "challenge/response" authentication systems[87] for e-mail) to intercept, and reduce the value to the sender of engaging in, abusive UCE.

VI. WAYS OF THINKING ABOUT THE UCE PROBLEM AND ITS POSSIBLE SOLUTIONS

Some of the difficulty in coming to grips with UCE may arise from the significantly different approaches that various observers and participants in the spam wars – even those clearly on the same general side in the spammer vs. anti-spammer arms race – take to some of the fundamental questions regarding UCE. The answers to these question vary based upon each analyst's view of what purpose the Internet and e-mail serve (or ought to serve), why (or even if) UCE abuse is a problem, who is to blame for that problem, and what solutions to this problem are both feasible and acceptable from a policy perspective.[88] Indeed, these divergent different analyses make it difficult even to define "spam." Such differing perspectives also inform the various

86. John Leyden, *US Anti-Spam Laws "Will Legalise Spam,"* THE REGISTER (Jan. 7, 2003), *available at* http://www.theregister.co.uk/content/archive/31506.html (citing Spamhaus contention that "around 200 individuals, most of whom are US-based, are responsible for around 90 percent of world's spam messages (or at least nine in 10 of those who can be traced, anyway). Several are based in Boca Raton, Florida, which has earned the unenviable reputation at the world's spam capitol."); News Release, *War On Spam: EU Calls For International Cooperation*, EUROPEAN UNION (Feb. 3, 2004), *at* http://www.eurunion.org/news/press/2004/20040012.htm (asserting that "[s]pam accounts for more than 50% of EU e-mail traffic, 80% of which is in English and 80% of which claims to originate in North America according to December 2003 figures.").

87. Such authentication regimes would require (before an e-mail was delivered) that the sender personally respond to a challenge automatically generated by the receiving party's server, with the required response being of a type impossible for automatic-mailing software to generate. Similar approaches would involve requiring a sender's name and return address to appear on a "white list" of senders trusted by the recipient, or implementing improved tracking and analysis of e-mail headers to detect the "true" originating address even when the header has been forged or 'spoofed.'

88. *Cf. generally* Philip Bobbit, CONSTITUTIONAL FATE (1982) at 25–28, 9–24, 39–58, 74–92, 93–119 (laying out six "modalities," or approaches to interpretation, through which disparate scholars have approached constitutional analysis (textual, historical, structural, doctrinal, prudential, and ethical), and suggesting that the conclusions drawn as to proper or desirable interpretation of constitutional meaning and policy may be influenced considerably by the specific mode of analysis applied).

approaches to making a significant dent in spam through legislative initiatives, regulation, litigation, or technological solutions. Below we set forth a few exemplary (and somewhat-simplistically characterized) "modalities" of thought that seem to have animated the perceptions and conclusions of various observers and participants in the spam wars as to what spam is, and what – if anything – can and should be done about it.

A. "Information Wants To Be Free"[89]

The Internet has long had a reputation as a haven for individualists and experimenters.[90] Many Internet pioneers and experts have been vociferous in their opposition to most forms of governmental incursion into the realm of electronic communication or commerce. Some reach this anti-regulatory standpoint from either a libertarian or classical liberal economic viewpoint,[91] and some from a more left-leaning concern with freedom of speech and communication.[92] It thus perhaps comes as no surprise that many proponents of a minimally-regulated Internet have not lined up behind any governmental approach to UCE control.[93] Indeed, some have

89. *See* Roger Clarke, *"Information wants to be free..."*, (Aug. 28, 2001), *at* http://www.anu.edu.au/people/Roger.Clarke/II/IWtbF.html (attributing the phrase's genesis to author Stewart Brand, ca. 1984); *but see* Cecil Adams, *Recent Columns*, The Straight Dope, *at* http://web.archive.org/web/19961230204507/http://www.straightdope.com/ (suggesting a limitation on the usefulness of this rallying cry as a practical policy tool: "Before you start penning missives complaining that there is only a year of [the author's] columns available and that 'information wants to be free,' please remember that this information actually wants to one day be bundled up and sold for $9.95 at a store near you.").

90. *See, e.g.*, Erik Jay, *Tales from the Internet: Part 1, Weapons of Misinstruction, Enter Stage Right* (Mar. 27, 2000), *at* http://www.enterstageright.com/archive/articles/0400internetp1.htm (noting that demographic data supported the perception of comparatively-early Internet users as disproportionately "libertarians, independents, and individualists," but cautioning against over-simplistic political characterizations of Internet enthusiasts).

91. *See, e.g.*, Paul Kapustka, *Anti-Tax Group Calls For Moratorium On VoIP Regulation*, INTERNETWEEK.COM (Apr. 7, 2004), *at* http://www.internetweek.com/breakingNews/showArticle.jhtml?articleID=18900527 ("[T]he National Taxpayers Union is asking for 'an explicit policy of forbearance of taxation and regulation on Internet telephony,' to better ensure that the growth of the nascent technology isn't hampered by taxes or regulations.").

92. *See, e.g.*, *Chilling Effects of Anti-Terrorism: "National Security" Toll on Freedom of Expression*, Electronic Frontier Foundation, *at* http://www.eff.org/Censorship/Terrorism_militias/antiterrorism_chill.html (criticizing federal efforts to regulate access to controversial Internet content in the name of national security and law enforcement, and speaking in support even of right-leaning website freerepublic.com in its federal copyright dispute with publishers whose articles freerepublic.com reproduced in connection with political commentary).

93. *See, e.g.*, the Electronic Frontier Foundation's *Spam (Junk E-Mail UBE) Archive*, *at* http://www.eff.org/Spam_cybersquatting_abuse/Spam/; Marvin J. Johnson, *A.C.L.U. Interested*

looked with skepticism on any broad treatment of UCE as a problem to be quashed, believing that such approaches may suppress the presumptively-favorable maximization of information exchange and threaten to legitimize other governmental intrusions on personal and economic liberty.[94] Some, indeed, wax elegiac about the liberating democratic potential of completely unregulated e-mail.[95] The ability to send anonymous, untraceable e-mails, using such spammer-beloved tactics as return address spoofing or anonymous "remailers" has even been specifically touted as a signal benefit of the electronic age (because of its potential, in non-commercial settings, to embolden legitimate criticism, complaint, and the identification of wrongdoing, as for instance an employee's revelations to the SEC of corporate misconduct by his superiors).[96]

Persons Memo: Analysis of S. 630, Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2001 or the CAN SPAM Act of 2001 (May 15, 2002), *at* http://www.aclu.org/FreeSpeech/FreeSpeech.cfm?ID=10361&c=84 (critiquing an earlier version of the Act).

94. *See, e.g.*, Steven Cousineau, *Libertarian Approaches to Addressing Spam*, THE LIBERTARIAN ENTERPRISE (June 24, 2002), *at* http://www.webleyweb.com/tle/libe179-20020624-09.html (rejecting a suggestion for regulating spam by imposing a taxing firewall to exact a *de minimis* (per message) charge on each outgoing Internet communications (which would arguably not significantly affect "legitimate" e-mail users but would pose a crushing burden to spammers sending millions of messages): "[T]he power to tax is the power to destroy. The only other government based alternative is laws that will probably be both ignored and ignorant. I still get a pile of spam and so far twenty (20) states have laws addressing spam Laws on the Internet to date have only worked where all of the participants agree on the necessity of following the law.").

95. *See, e.g.*, John "Birdman" Bryant, *A Libertarian Defense of Spam*, *at* http://www.thebirdman.org/Index/Lbtn/Lbtn-Spam.html:

> Let's put it this way: Spam is the key to freedom on the Net. Spam is the free exchange of ideas – the modern town square – the new Liberty Tree of the American nation, and indeed, of the entire world. . . . Spam is how people get connected, and thus spam is how these connections will develop into the great convolution-filled cerebrum of Gaia.
>
> . . .
>
> The bottom line, then, is that spam is not the problem. Rather, the problem is the controlled market in which it occurs, and the eagerness of Big Ugly Government types to use the 'issue' of spam to get their greasy regulatory fingers around the throat of the greatest boon to freedom in the history of the world.

96. *See, e.g.*, Andre Bacard, *Anonymous Remailer F.A.Q.*, Nov. 15, 2003, *at* http://www.andrebacard.com/remail.html:

> Why would YOU use remailers? Maybe you're a computer engineer who wants to express opinions about computer products, opinions that your employer might hold against you. Possibly you live in a community that is violently intolerant of your social, political, or religious views. . . . Perchance you're a whistle blower afraid of retaliation. Conceivably you feel that, if you criticize your government, Big Brother will monitor you. . . . In short, there are many legitimate reasons why you, a law abiding person, might use pro-privacy email systems.

It is perhaps fitting that the ideological rallying cries of the "free information" approach to Internet and e-mail regulation (in which freedom of access and exchange is viewed as a near-paramount good), once enunciated by serious theorists of differing political stripes, flowed with nearly friction-free rapidity into the minds and hands of UCE purveyors. It may be true that the Cato Institute or ACLU membership status of some spammers is subject to doubt, and that their respective acquaintance with the heights of von Mises' economic theory, or the other philosophical elevations reached in libertarian warnings against "Big Ugly Government," would prove somewhat limited. But UCE purveyors, legitimate and otherwise, have bowed to no man in their enthusiastic embrace of "free information"-based analyses of policy issues concerning regulation of e-mail.[97]

---

97. *See* Stefanie Olsen, *Judge ties antispammer's hands*, CNET NEWS (May 11, 2004), *at* http://news.com.com/2100-1024_3-5210518.html (reporting on temporary restraining order entered by Northern California federal district court, prohibiting leading anti-spam website SpamCop and its parent IronPort Systems, on an interlocutory basis, from offering their "blacklisting" and spam reporting techniques against notorious UCE purveyor Scott Richter and his company OptInRealBig.com, on the asserted grounds that SpamCop's actions interfered with Richter's business and caused his ISP to block his company's e-mail. In a claim that would be astonishing coming from anyone outside the ranks of unrepentant spammers, Richter also invoked CAN-SPAM as an affirmative basis for granting relief to *him*, on the bizarre theory that SpamCop's use of anonymized spam reports (employed for the purpose of preventing spammers from redoubling their spam efforts against recipients who verified their identity by complaining about alleged spam) somehow abetted violations of CAN-SPAM by inhibiting the ability to remove complaining recipients from mailing lists); *see also* Peter A. Johnson, *Preserving The Promise of The E-mail Marketplace: An Economic Assessment of The Proposed Federal DO-NOT-E-Mail Registry*, Direct Marketing Association (Mar. 31, 2004), *at* http://www.the-dma.org/antispam/final.pdf, p.5 ("New firms increase competition that drives down prices for consumers and accelerates the introduction of productivity-enhancing products and procedures. Legitimate commercial e-mail is uniquely positioned to reduce barriers to entry because of its low per-contact cost (making it flexible enough for small marketing campaigns) and because of its disproportionately high return on investment per contact, which facilitates rapid customer acquisition—i.e., rapid business growth."); David Leonhardt, *If Spam Vigilantes Break Out of Cyberspace*, *at* http://www.stickysauce.com/articles/advertisingpromotion/if_spam_vigilantes_break_out_of_cyberspace.html (providing commercial e-mailer's dystopian, if sub-Orwellian, scenario of a heavily-regulated future in which senders of e-mail face various Draconian sanctions for actions as simple as sending a resume to apply for a job with a company: "'But doesn't every exchange begin with an unsolicited message,' I asked. 'Welcome to the post-Internet world. The greatest communications tool of all time ended communications forever.' 'But what can we do about it?' I wanted to know. 'I don't know about you,' he said as he slipped into his jacket. 'But I'm off to the freedom-of-speech bureau to report an unsolicited conversation. They should be here soon to staple your mouth shut.'"); *see also* Washington v. Jason Heckel, d/b/a Natural Instincts, 24 P.3d 404, *cert. denied*, 122 S. Ct. 467 (2001) (reversing trial court decision which had accepted defendant's argument that Washington State's then-in-force anti-spam law violated the Interstate Commerce Clause by requiring UCE senders to determine the state where each e-mail recipient resided; the Washington supreme court, however, was less moved by defendant's arguments regarding unfair restraints on commerce,

While this perspective has deep roots, its embrace by direct marketers and other spammers should give everyone pause. Clearly, some degree of "free information" analysis informed the CAN-SPAM Act, which does little if anything to intrude on the free marketplace of e-mail. This perspective, however, ignores the harsh realities of spam and the independent dangers that it poses to Internet culture and Internet infrastructure.

B. "The Market Has Failed"

Even Internet veterans, who might in other respects espouse the rugged individualist view of the Internet as a medium whose potential best thrives when left to the grassroots ingenuity of its atomistic, distributed participants, seem less than convinced about the benefits of a totally unregulated Internet and e-mail regime. Some believe that bad information (such as spam) threatens to drive out the good information whose free exchange was one of the exciting, and potentially-liberating, promises of the Internet frontier. A vigorous liberal economics-based embrace of the Internet and e-mail as liberating, and profit enhancing, tools in a free market of information, ideas, and goods and services does not imply wholesale acceptance of a rule-free marketplace. Even ardent free market theorists may accept that not all markets are purely efficient, and that less-than-efficient markets are subject to failure.

From this perspective, rational regulation of the e-mail "market" is entirely appropriate. How that regulation would occur, however, and the extent of that regulation would depend on the perceived cause of the market breakdown.

There are at least four generally-accepted causes of market failures: (a) imperfect competition (i.e., the ability for monopolies to exist on either side of the market transaction); (b) public goods (a good which can only be provided, usually by the government, on a freely-accessible basis to any who wish to use it); (c) asymmetric information (i.e., the transaction parties do not have equal access to information that would influence their willingness or ability to consider rationally, and enter into for a fair price, the proposed transaction); and (d) interference of externalities in the market (i.e., one or more market participants can impose a cost on another without giving up anything of corresponding economic value, or can take

---

and after reversing the trial court's invalidation of the statute, remanded for trial court proceedings that ended in a substantial monetary verdict against defendant (*see* Michael Chissick, *Putting a price on spam*, INTERNET MAGAZINE (Mar. 2003)).

something of economic value while imposing the costs thereof on those who do not benefit from the transaction).[98]

The Internet as historically and currently constituted, and commercial e-mail in particular, arguably are subject in a significant degree to all but one of these causes of potential market failures (the exception being imperfect competition, given that individuals' cheap and ready access to Internet and e-mail facilities arguably render it difficult for any one Nigerian, for instance, to corner the market in fictitious government funds supposedly sequestered by a deposed relative).

The Internet's origin's as a network (originally, under the Defense Department-sponsored ARPANET) for communication of technical information among defense researchers, including the ability, implemented by the 1970s, to exchange person-to-person mail-type electronic messages between the researchers, may constitute a fundamental source of the difficulties encountered in fighting spam today, even as the Internet has moved far beyond its origins as a government-sponsored information exchange to encompass and enable largely-private interests.[99]

Many of the basic characteristics and protocols for Internet information exchange, and the assumptions as to how e-mail should operate, have their origins in the era when Internet and e-mail were provided as public goods and their users were presumed to be productive researchers. The maximization of such researchers' free information exchange was viewed as enhancing the public interest, even if it did not directly defray the costs incurred by the network provider(s).[100] For instance, there was no reason for the government-

98. *See, e.g.*, http://pages.stern.nyu.edu/~gsimon/ProfResp/MARKETFAILURES.pdf. (some economists would also point to taxation as a market-distorting factor, but to date the Internet and e-mail have not been subject to significant taxation, so we do not examine this factor).

99. *See generally* Ian R. Hardy, *The Evolution of ARPANET email*, Thesis (Univ. Cal. Berkeley) (1996), *at* http://www.ifla.org/documents/internet/hari1.txt.

100. *See, e.g.*, Brad Templeton, *Reflections on the 25th Anniversary of Spam*, *at* http://www.templetons.com/brad/spam/spam25.html (detailing first recorded large-scale UCE sent over ARPANET, and noting that the only barriers then deemed necessary to prevent such misuse were voluntarily-observed "acceptable use policies" among the small community of ARPANET participants); *see also* Bills Digest No. 45 2003-04, Spam Bill 2003 (Australian Parliament), *at* http://www.aph.gov.au/library/pubs/bd/2003-04/04bd045.htm (noting, in legislative history of anti-spam bill, that ARPANET was intentionally developed on a decentralized basis, with no single network administrator responsible for administration of the entire network, partly in order to increase its robustness and resistance to disruption in the event of nuclear attack or other localized network failure – a technical artifact that continues to make centralized regulation of the Internet a difficult task).

enabled ARPANET to develop strict technical protocols for preventing spoofing or other alteration of source addresses for e-mail, at least at a time when access to the system was limited to government-approved researchers.[101] Additionally, certain crucial functions of Internet governance (such as registration of, and dispute resolution as to, domain names) continue to be delegated by national governments to quasi-governmental bodies, who are mandated to facilitate Internet service for the general public. However, such bodies enjoy considerable discretion (free, as would a governmental agency be, from market pressures) as to how they carry out these functions.[102]

The ready ability of e-mail senders to disguise the origin of a message or to falsify the identity and contact details of a registrant for a domain whose services are advertised by spam, provides a simple instance of a second potential cause of market failure for commercial e-mail transactions. That is, recipients of commercial e-mail will often be in an asymmetric, and clearly inferior, position vis à vis the originator of UCE as regards commercially-important details of the transaction. Marketers have an incentive to be promiscuous in spreading their messages to the four winds. It matters little where these messages land, so long as some recipient can be enticed to buy

---

101. *See* Templeton, *supra* note 100.

102. *See, e.g.*, Caslon Analytics Profile: ICANN and the UDRP (Oct. 2002), *at* http://www.caslon.com.au/icannprofile5.htm (analyzing the role of the Internet Corporation For Assigned Names And Numbers ("ICANN"), a private body authorized by the U.S. and other governments to supervise Internet Protocol (IP) address space allocation through its authorized independent domain registrars, protocol identifier assignment, generic (gTLD) and country code (ccTLD) Top-Level Domain name system management, and root server system management functions (all functions originally performed under U.S. Government contract by the Internet Assigned Numbers Authority (IANA) and other entities):

> [Some activists] argue that key governance decisions about central resources and operations are being made by agencies such as ICANN that have quasi-governmental powers, that operate on a global level but lack the accountability of government. They also argue that there is real need to focus the attention of civil society on seemingly technical issues determined by those agencies.

ICANN has recently been criticized specifically for lack of accountability and effective oversight on spam issues, based on its alleged failure to require authorized registrars of domain names (and their affiliated mailservers) to implement reliable verification of registrant's "WHOIS" contact information and other particulars so that spammers can be readily traced and pursued based upon their domain registration records. Such a failure would have significant implications in view of the fact that many spammers register numerous domains using bogus contact information in order further to mask themselves from public view or complaints. *See* Jim Wagner, *ICANN Reports On WHOIS Inaccuracies*, internetnews.com (Mar. 31, 2004), *at* http://www.internetnews.com/xSP/article.php/3334181.

the marketer's product at his asking price.[103] Conversely, numerous pieces of information that would normally be crucial to a prudent consumer's purchase decision can be concealed – or more often, falsified – by merchants operating behind the anonymity of the Internet and effectively-anonymous e-mail.[104] Such manipulated, concealed, and falsified information can include the identity and reputation of the merchant; the nature and reliability of the advertised product; the product's ability to perform the advertised functions; and the location and availability of the merchant if the customer requires customer service or remedial action for product failure.

Especially as to products or services that may have a strong emotional appeal to a customer (such as dating services or romantic adjuncts), or that may be relatively unavailable through more conventional and transparent channels (prescription drugs, cable descramblers, and other products of dubious legality), or that make not-readily-falsifiable claims of long-term benefit to the consumer (such as business schemes), a customer's strong desire to obtain the product or services in question may win out over sober second thoughts when there is no ready or cost-efficient way to test or look behind the multiple unproven assumptions contained in the merchant's proposition. Such impulse purchasing could prove problematic even if the product exists and has traits roughly according with those described in the UCE, and the merchant can be trusted to deliver it, because not every consummated transaction is a prudent transaction.

Finally, externalities, perhaps the most common cause of market failures, abound in the mass-mailed electronic commercial solicitation market. The single most notable externality involved in UCE arises out of the cost structure (or rather, lack of one) for sending e-mails. Many have noted that the current system of e-mail provision makes it possible for an e-mail sender to dispatch millions of e-mails without incurring substantially greater costs than if he sent a few hundred[105] –

---

103. Accordingly, the most important, and perhaps the only, piece of information that a UCE marketer needs to ascertain with regard to his customer is that the customer's promise to pay for his cable descrambler or growth hormone actuator or mortgage refinance application, as the case may be, can be reliably converted into cash in the marketer's pocket. But this information can be obtained fairly readily and cheaply through numerous credit card verification and fulfillment systems or other Internet-enabled payment mechanisms.

104. *See supra*, note 8.

105. *See, e.g.*, John Leyden, *The economics of spam*, THE REGISTER (Nov. 18, 2003), *at* http://www.theregister.co.uk/2003/11/18/the_economics_of_spam/ ("[S]pam makes economic sense, despite miniscule response rates, because spam can be sent at 'virtually no cost to spammers.' Spam, unlike conventional junk mail, is growing exponentially because it costs

indeed, e-mail is often regarded at the margins as an essentially free form of communication.

Of course, the servers and bandwidth necessary to transmit huge volumes of UCE are not, even in an era of cheap computing power, free at all. Rather, the costs associated with transmission and receipt of millions of spam messages (not to mention the costs of monitoring and combating UCE message through such means as spam filters and virus checkers) are simply localized at other nodes of the UCE loop – *viz.*, at the ISPs,[106] network infrastructure providers, and UCE recipients.[107]

The negative externalities imposed by spam go beyond simply the cost of processing, and combating, UCE. Many of the products and services most popularly advertised through UCE are – charitably put – of unproven value. They may in more than a few instances fail to deliver upon the expansive, often creatively-phrased,[108] promises contained in the come-on to the consumer. Even the promulgators of UCE who purport to operate on a "legitimate" basis have been forced to concede that the proliferation of simply fraudulent UCE is

---

virtually nothing to send and all the costs of dealing with spam are dumped on its recipients. . . . [R]esponse rates to bulk commercial email is less than 0.005 per cent. That means that a typical email message appeals to 50 people and annoys 999,950."); *see also* Andrew Leung, *SPAM: The Current State*, Telus Corporation (Aug. 8, 2003), *at* http://www.telusinternational.com/Download/spam.pdf, p.7-8 (noting that in the currently-prevailing business model in which outgoing e-mail is not generally subject to strict volume limits or charged to senders on a per-unit basis, and in which spammers can use techniques such as open-relay hijacking to avoid any limits that do exist, spammers encounter essentially no incremental financial disincentive not to maximize the volume of solicitations dispatched).

106. *See, e.g.*, Christina Torode, *Spam Leads To High Costs For ISPs*, INTERNETWEEK.COM (Apr. 28, 2003), *at* http://www.internetwk.com/breakingNews/showArticle.jhtml ?articleID=9400084 ("Spam costs these ISPs in many forms: the need for an antispam staff; additional storage, bandwidth and software requirements; the need for resources to develop homegrown solutions and additional man-hours to handle reconfigurations; and lawsuits brought both against spammers and against the ISPs. . . . What's more, research firm Gartner estimates that, on average, an ISP with 1 million users spends $7 million a year fighting spam."

107. *See, e.g.*, Leung, *supra* note 105, at 9 (estimating that, in the 2001-2003 time period, individual companies lost approximately $8.9 billion, in aggregate, annually from spam, about half of the estimated total coming from lost worker productivity in reading and discarding or attempting to unsubscribe from spam messages, and the other half in purchasing more powerful servers and greater hard drive space, increased network bandwidth, and help-desk support to company users and customers for spam and relay hijack incidents).

108. *See, e.g.*, Rick Conner, *A gallery of classic spam*, (Mar. 23, 2004) *at* http://www.rickconner.net/spamweb/classicspam.html; *see also* Spam Examples, *at* http://www.linuxfocus.org/common/src/article279/spam_samples.html.

threatening consumer confidence in all e-mail solicitations, and may put a serious crimp in the potential growth of online commerce.[109]

Not all externalities of UCE abuse are purely negative (at least from the standpoint of some of the UCE's recipients). Some spammers may actually deliver essentially what they advertise – say, prescription drugs and narcotics not otherwise readily available to consumers with no medical need for them, or who seek to circumvent drug company pricing policies by ordering drugs (or their unauthorized generic equivalents) from another jurisdiction. Thus, a comparatively small number of UCE recipients who respond favorably to solicitations for such drugs (or for illegal cable descramblers, or pornography) may well enjoy (from their standpoint) the benefit of access to products or services otherwise not readily available to them. But millions of other recipients (and ISPs, and so on) are forced to pay the price for those few consumers' "benefits," in the form of dealing with untargeted mass UCE solicitations as to which the vast number of recipients do not wish to avail of the "positive" externality being proffered by the solicitor.

Accordingly, a market failure modality of analyzing the problems of UCE could plausibly point to numerous structural flaws in the current structure of, and economic model for, distribution and fulfillment of e-mail, and in particular, UCE. From this standpoint, the fundamental problem is not necessarily that free exchange of information and goods is a bad thing. Rather, a "market failure" proponent would be likely to advocate for those technical and regulatory changes that offer the potential to eliminate unhelpful historical artifacts in the Internet and e-mail business model and to counterbalance the other arguably-skewed economic factors that threaten to negate the Internet's great potential as a global, efficient market in information, goods, and services.

C. "But What About The Children?"

The legislative history and text of the CAN-SPAM Act, and many of the proposed state regulations, placed considerable emphasis on the transmission of pornographic images and sexually-oriented

109. *See, e.g.*, H. Robert Wientzen, *TACKLING THE SPAM ISSUE: The DMA's answers to one of the nation's toughest questions*, DIRECT MARKETING ASSOCIATION, *at* http://www.the-dma.org/memberguide/tacklingspam.shtml ("Unfortunately, in the public arena, some of those negative sentiments about spam are impacting legitimate e-mail marketing. I've heard concerns from DMA members about falling response rates and overly aggressive spam filters. And given the unprecedented growth rates we've seen from spammers just this year, I fear we've only begun to scratch the surface.").

solicitations as one of the principal evils of unchecked UCE. Indeed, many who would otherwise be loath to regulate e-mail in any way would jump at the chance to regulate pornography.

Certainly, a significant amount of UCE relates to adult-oriented services or products, often advertised using graphic language and explicit photographs. The indiscriminate nature of spam solicitation has meant that e-mail users (including children) who might otherwise never be directly exposed to adult-oriented content have found it, to their amazement, splashed across their computer screen upon opening an e-mail message. While pornography-oriented solicitations in fact appear to make up only a small minority of all UCE,[110] their graphic and controversial nature has played a disproportionately heavy role in stoking anti-spam fervor.[111]

More broadly, concern for public health and morals, and the perceived threats posed to both by unregulated UCE, have supplied motivation to a substantial segment of the anti-spam movement. Most UCE is, after all, deceptive on some level – including, often, the

110. *See, e.g.*, Lucy Sherriff, *Sex, drugs and cans of spam*, THE REGISTER (Feb. 19, 2004), *at* http://www.theregister.com/2004/02/19/sex_drugs_and_cans/ (citing statistics from e-mail filtering firm Clearswift, showing that pornography-related e-mail constituted only 22% of spam in January, 2004, as compared to pharmaceutical solicitations, which accounted for almost 43% of all spam); *see also Spam Statistics*, BRIGHTMAIL, *at* http://www.brightmail.com/spamstats.html (providing statistics from spam filtering company Brightmail suggesting that only 15% of UCE in March, 2004 was adult-oriented). As any statistics regarding spam are based upon representative sampling of a particular e-mail recipient population, it is not always clear how reliable and consistent such statistics are; for instance, the Brightmail statistics cited above estimated that health or pharmaceutical-related spam made up only 7% of the total volume in March, 2004, which is wildly at odds with Clearswift's estimate that this category accounted for almost half of all spam. *See id.*

111. *See, e.g.*, Press Release, *Schumer, Christian Coalition Team Up To Crack Down On Email Spam Pornography* (June 12, 2003), *at* http://www.senate.gov/~schumer/SchumerWebsite/pressroom/press_releases/PR01782.html (announcing self-described "odd couple" alliance between liberal Senator Charles Schumer and conservative Christian Coalition in support of CAN-SPAM Act, citing statistics regarding widespread exposure of children to e-mail based pornography (as well as conflating the non-e-mail-related problem of solicitation of children by chat-room predators), and characterizing CAN-SPAM largely in terms of its intended role in preventing pornographic e-mails: "The avalanche of pornography being sent to kids by spammers makes checking email on par with watching an X-rated movie."); *see also* Deborah Fallows, *Spam: How It Is Hurting Email and Degrading Life on the Internet*, PEW INTERNET AND AMERICAN LIFE PROJECT (Oct. 22, 2003), p. 29, *at* http://www.pewinternet.org/reports/pdfs/PIP_Spam_Report.pdf :

> There is a special place in Hell for pornographic spam. Throughout this study, email users' reactions to spam containing adult content and pornography have stood out. When asked to identify the type of *content* that bothers users most, once again pornography exceeds all others, by nearly four times more than any runner-up. People, and especially women and parents, hate it.

substantive description of the goods or services being offered.[112] Quack herbal nostrums may have unexpected, and serious, side effects not disclosed in the unregulated advertisements that tout them.[113] According to Brightmail, an estimated twenty percent or more of UCE consists of solicitations for investment in various financial products, or simple stock tips touting over the counter stocks; another seven percent consists of outright scams, such as the infamous Nigerian '419' scheme.[114] A final five percent involves "phishing" attacks disguised as e-mail from legitimate companies and intended to inveigle recipients into supplying personal information such as credit card numbers for "verification."[115] The financial risks to e-mail recipients from actually availing of the purported opportunities or solicitations contained in such e-mails are substantial.

Finally, even as to solicitations that are "legitimate" from a commercial perspective (i.e., that accurately describe and deliver goods and services largely as promised), there may be additional public policy problems perceived with allowing such transactions to take place. The anonymity (for both seller and buyer) afforded by e-mail based solicitations has tended to skew the product mix for UCE-advertised goods to those products that (like pornography) may be in high demand but as to whose purchase consumers might otherwise encounter legal or social barriers. Many observers will likely embrace, as valuable safeguards, existing legal and community-mores-based barriers to obtaining, say, prescription painkillers or tranquilizers for self-medication,[116] or to purchasing cable television

112. *See, e.g.*, Fallows, *supra* note 50 (reporting random sampling of 1000 pieces of UCE by the FTC, which found that 66% of the e-mails contained false or misleading information in the body or the header/subject information, with 44% of the samples containing false or misleading statements, claims, or characterizations in the sales pitch itself).

113. *See, e.g.*, Glenda Patton, *The dangers of drugs and herbal interactions*, *at* http://il.essortment.com/drugandherbal_rgyv.htm.

114. *'Nigerian' e-mail scam netted millions: prosecutors*, GLOBEANDMAIL.COM (Oct. 31, 2003), *at* http://www.globetechnology.com/servlet/story/RTGAM.20031031.wscam1031/BNStory/Technology/ (describing charges brought against scammer who secured over four million Canadian dollars using e-mail solicitations in which he purported to have access to former Nigerian president's sequestered assets).

115. *See Spam Statistics*, Brightmail, *at* http://www.brightmail.com/spamstats.html. The Clearswift breakdown of spam for the same month, March, 2004, once again contains significantly different estimates from those of Brightmail. Though Clearswift cites a similar number to Brightmail (26%) as to financial solicitations, it sets a much lower estimate than Brightmail on the proportion of scam and phishing-related e-mails (classing just 0.4% of UCE as unadulterated scams).

116. *See, e.g.*, Marc Kaufman, *Crackdown on Prescription Abuse: U.S. Officials Want Better Monitoring, Control of Painkillers*, WASHINGTON POST (Mar. 2, 2004), *available at*

descramblers.[117] These observers may also tend to believe that unregulated electronic commerce poses threats not only to unwitting victims of scams and misleading advertisements, but also to weak-willed buyers who are all too successful in consummating transactions whose effect is deleterious to their own, or society's, well-being.

Approaches to UCE that are inspired by a public health and morals view of spam will likely continue to focus on legislative provisions (such as those in the CAN-SPAM Act) requiring the identification of adult-oriented materials (so that they may readily be filtered or rejected), along with the other provisions of CAN-SPAM (which could reduce the perils posed by spam that, while non-sexual in nature, is still perceived as posing health, financial, or other risks to individual consumers or to society). Stricter enforcement of existing, non-e-mail-related, laws proscribing the underlying bad conduct being promoted by UCE[118] is also likely to form a parallel route of attack by those who view threats to consumer health and welfare and public safety as a principal gravamen of spam.

Expecting industry to police itself in a potentially lucrative marketplace may seem a low-percentage approach in any context, but if appropriate pressure can be brought to bear at key points of the supply chain, "legitimate" industry players may also be persuaded to cooperate in limiting the ability of spammers to subvert public policy.[119]

---

http://www.washingtonpost.com/wp-dyn/articles/A20863-2004Mar1.html (noting ready online availability of opiates and other prescription drugs without prescription).

117. *See, e.g.*, Jim Lawley, *Despite sellers' claims, cable descramblers are illegal*, DECATUR DAILY (May 19, 2003), *at* http://www.decaturdaily.com/decaturdaily/livingtoday/030519/cable.shtml (noting prevalence of e-mail solicitations for unauthorized descramblers used to obtain free access to cable television programming).

118. Such as obscenity, *see How to Report Possible Violations of the Federal Obscenity Laws*, Morality In Media, *at* http://www.obscenitycrimes.org/complaint/offline_report_fed.cfm; improper prescription drug trafficking (21 U.S.C. §§ 353, 822, 829, 841); and illegal gambling (18 U.S.C. § 1084).

119. For instance, manufacturers of controversial drugs such as anabolic steroids and prescription painkillers have, following public outcry, adopted stricter regulation of the downstream market for their products to prevent diversion and abuse. *See, e.g.*, *Action Plan to Prevent the Diversion and Abuse of OxyContin®*, United States Drug Enforcement Administration, *at* http://www.deadiversion.usdoj.gov/drugs_concern/oxycodone/abuse_oxy.htm ("[Manufacturer] Purdue Pharma has been encouraged to develop a balanced marketing strategy that ensures appropriate use of OxyContin®."); *see also* Press Release, *ASACP Received Over 2700 Suspect Child Pornography Reports in December '02 Compared to 1200 in December '01*, (Jan. 2003), *at* http://www.asacp.org/press/press0103b.html (detailing efforts of adult website industry group ASACP to identify and report to authorities any parties sending e-mail solicitations involving child pornography).

Any attempt to regulate e-mail based upon its content raises the specter of constitutional concerns – concerns that may be heightened in the context of the "health and morals" approach to spam. Critics and laws adopting this modality of viewing and attacking spam are pretty clearly motivated, in part, by disagreement with the underlying content of the message that the UCE promulgator is sending. The government's ability to place reasonable restrictions on commercial speech, however, is well-established.[120] The constitutionality of anti-spam laws may be further bolstered by the inability of many spammers to meet a threshold requirement for invoking commercial free speech defenses – namely, that the speech for which protection is sought pertains to lawful activity and is not misleading.[121] Still, past governmental attempts at regulating speech, specifically in the online context, have not fared uniformly well.[122] Even the limits on adult-oriented e-mails imposed by the CAN-SPAM Act are under attack in some quarters as constitutionally infirm.[123]

E-mail has exposed consumers to new opportunities for information and commercial transactions; but not all available information, and not all possible transactions, will conduce to the individual or collective good. Views will vary on how tightly commercial speech needs to be regulated in the context of e-mail. But it seems inevitable that UCE policy will continue to be driven in significant part by those who believe that consumers' health, safety, and morality need to be protected from the blandishments of e-mail

120. *See* Central Hudson Gas & Electric Corp. v. Public Service Commission, 477 U.S. 557, 566 (1980) (applying a four part analysis to restrictions on advertising, including determining: (1) whether the advertisement concerns lawful activity and is not misleading; (2) whether the government interest in regulating the advertisement is substantial; (3) whether the restriction directly advances the governmental interest asserted, and finally, (4) whether the restriction is more extensive than is necessary to serve that interest).

121. *Id.* ("[T]here can be no constitutional objection to the suppression of commercial messages that do not accurately inform the public about lawful activity. The government may ban forms of communication more likely to deceive the public than to inform it, or commercial speech related to illegal activity.") (citations omitted).

122. *See* Ashcroft v. ACLU, 122 S. Ct. 1700 (2002) (upholding injunction against enforcement of Child Online Protection Act and its prohibitions on electronic communications containing "material harmful to minors"); Reno v. ACLU, 521 U.S. 821 (1997) (holding key provisions of Communications Decency Act unconstitutional).

123. *See, e.g., Comments of the Center for Democracy and Technology on Notice of Proposed Rulemaking: Proposed Mark for Sexually Oriented Spam*, (Feb. 17, 2004), *at* http://www.cdt.org/speech/spam/20040217cdt.shtml (arguing that the FTC ought not to implement a requirement of a subject-line label identifying all adult-oriented UCE as such, even though CAN-SPAM clearly sets forth such a requirement, and instead arguing for an alternative approach not subject to the perceived constitutional problems of the labeling procedure prescribed by the statute).

solicitations for harmful or fraudulent products – as well as from their own credulity and venality.

D. "Western Science Is So Wonderful"[124]

To some, weary or wary of legislative attempts to stop spam, or simply more enamored of technological solutions to a technology-facilitated problem, victory in the UCE wars will come through superior technological firepower, not through any legal or regulatory approach. After all, the ease with which spammers operate is, in part, a technological artifact of the open communications framework set up for the small ARPANET community. Surely, some reason, the technological loopholes that allow spammers to flourish can be closed by the combined technical skills of computer science companies, institutions, and public-spirited hackers.[125]

Certainly there are significant technical weaknesses in the current e-mail infrastructure. Minimizing the ability readily to spoof return address information comes to mind as one obvious (if not necessarily easy) step to limiting the anonymity (and thus lack of accountability) of UCE originators. It has ranked high among the proposed technical solutions to spam.[126] A number of technical

---

124. Cordwainer Smith, *Western Science Is So Wonderful*, *in* IF, DECEMBER 1958 79–89 (Damon Knight ed., 1958).

125. *See, e.g.*, Hanah Metchis, *Technology, Not Regulation, Takes a Bite out of Spam*, Competitive Enterprise Institute (Apr. 30, 2003) ("[I]t's not surprising that innovation in technological anti-spam solutions is taking off at incredible rates. . . . This evolving variety of approaches is more likely to alleviate the problem than Congressional solutions."); Scarlet Pruitt, *In Search of the Perfect Spam Filter: Techies immerse themselves in spam to craft a filter that renders mass e-mail marketing ineffective (and undesirable)*, PCWORLD (Jan. 17, 2003), *at* http://www.pcworld.com/news/article/0,aid,108859,00.asp (noting spam filter creators' belief that "if there is widespread adoption of filters that are accurate enough to make spamming economically prohibitive, the problem will cease without the need for legislation or other measures."); *Gates: Spam To Be Canned By 2006*, CBSNEWS.COM (Jan. 24, 2004), *at* http://www.cbsnews.com/stories/2004/01/24/tech/main595595.shtml (quoting Microsoft Corp. chairman Bill Gates as promising that "Two years from now, spam will be solved" by technological measures).

126. *See, e.g.*, *Caller ID for E-Mail Technical Specification*, MICROSOFT (Feb. 24, 2004), *at* http://www.microsoft.com/mscorp/twc/privacy/spam_callerid.mspx (outlining Microsoft proposal to address domain spoofing by verifying that each e-mail message originates from the Internet domain that it purports to); *The Absolute Ultimate Spam Protection*, GEEK NEWS CENTRAL.COM (Dec. 9, 2003), *at* http://www.geeknewscentral.com/archives/001985.html (reporting favorably on proprietary spam elimination program WCSAP, whose provider notes that the program employs anti-spoofing verification technology because "[p]art of the problem is that spammers have exploited certain loopholes in the email SMTP [Simple Mail Transfer Protocol basic Internet e-mail standard] technology . . . . WCSAP [becomes] essentially an SMTP standards compliancy testing software."); *A Plan for No Spam*, at p. 13, VERISIGN (2003), *at* http://www.verisign.com/resources/wp/spam/no_spam.pdf ("Detecting false sender

approaches to authentication of sender identity exist. These proposals include "passive" schemes largely transparent to the sender and recipient of the e-mail (such as improved tracking of SMTP and DNS (Domain Name Server) routing information). Other suggested solutions involve "active" approaches requiring some action or selection by sender or recipient. Such actions could include comparing originating e-mail addresses against a "whitelist" of trusted originating domains to which received e-mails will be compared, or employing "challenge-response" protocols requiring that the sender execute some confirmation step or routine (presumably, a routine not readily performed by automated means) before the message is delivered.

E-mail filters have also attracted considerable attention in the anti-spam world, and probably constitute the most important currently-implemented technological measure for spam control. Early filters were static rule-based programs that applied periodically-updated decision rules based upon a finite set of known characteristics of sampled spam.[127] More sophisticated Bayesian filters have recently come on the market. Bayesian filters search for patterns of word usage in a user's received e-mails (and their headers) and classify as spam those e-mails showing patterns suspiciously close to those of known spam, in a manner akin to simple rule-based filters.[128] But Bayesian filters also offer the promise of dynamic detection rules. That is, the filters can be written so as to "learn" incrementally, in a form of artificial intelligence ("AI"). As the corpus of inspected e-mail for a user or group of users grows larger, certain terms and patterns are determined likely to be characteristic of spam, and others characteristic of legitimate e-mail of a particular user, so that weighted spam-screening routines can be applied based on such

addresses would be a simple task but for the fact that the SMTP protocol allows a sender to forge a message that purports to come from any sender.").

127. Paul Graham, *Stopping Spam*, http://www.paulgraham.com/stopspam.html (last visited May 25, 2004).

The main disadvantage of rule-based filters is that they tend to have high false positive rates – often as high as .5%. Another disadvantage is that the rules are static. When spammers learn new tricks, the filter's authors have to write new rules to catch them. And because rule-based filters are static targets, spammers can tune their mails to get past them. Sophisticated spammers already test their mails on popular rule-based filters before sending them. In fact, there are sites that will do this for free.

128. *See, e.g.*, Paul Graham, *Will Filters Kill Spam?*, (Dec. 2002), *at* http://www.paulgraham.com/wfks.html ("What's going to happen as this new generation of spam filters get delivered to end-users? The most exciting possibility is that they may make spam go away.").

patterns.[129] Although originators of Bayesian filters claim impressive spam-blocking results,[130] such filters are not without their weaknesses. There exists the risk of "false positives," which leads to rejection of legitimate e-mail.[131] There is also the possibility that spammers will, as they already appear to be attempting, tailor the text of their e-mails to include many randomly-generated "innocuous" words and phrases in an effort to give the appearance of legitimate e-mail when scanned by the filter.[132]

A more aggressive technical approach to spam-fighting arises out of the hacker fringe of the programming world, and consists of direct action (or as some would put it, vigilantism) against spammers, aimed at interfering with their ability to conduct their business profitably. Blacklists that are distributed publicly, for use by ISPs and others in blocking all e-mail from known spam-originating domains, represent a comparatively mild form of direct action. But even blacklists have faced challenges from UCE originators alleging

---

129. *See, e.g.*, Heinz Tschabitscher, *What You Need To Know About Bayesian Spam Filtering*, ABOUT.COM ("[T]he message can be used to train the filter further . . . . Using this auto-adaptive technique, Bayesian filters can learn from both their own and the user's decisions (if she manually corrects a misjudgment by the filters). The adaptability of Bayesian filtering also makes sure they are most effective for the individual email user. While most people's spam may have similar characteristics, the legitimate mail is characteristically different for everybody.").

130. *See, e.g.*, Paul Graham, *Better Bayesian Filtering*, (Jan. 2003), *at* http://www.paulgraham.com/better.html (claiming 99.5% success in detecting spam using author's Bayesian filter).

131. *See, e.g.*, *Bayesian Filtering: The Spam Fights Back*, THE FISHBOWL (Sep. 4, 2003), *at* http://fishbowl.pastiche.org/2003/09/04/bayesian_filtering_the_spam_fights_back (discussing problems with false positives in Bayesian filtering).

132. *See id.* ("[i]f we had a more sophisticated linguistic filter, it wouldn't be hard for spammers to come up with a program that generated random, but grammatically correct sentences"); Graham, *supra* note 127 (theorizing that the use of completely innocuous random text, coupled with a URL to the spammer's website, could defeat even some sophisticated Bayesian filters); *see also* Bruce Bower, *Mind-Expanding Machines*, SCIENCE NEWS (Aug. 30, 2003), at 136 (reporting on dissidents within the AI community who "dismiss[] the influential Turing Test [which evaluates the success of machine intelligence by testing whether the machine is capable of behaving indistinguishably from a person] as a guiding principle for AI research," based in part on AI research's "failure to create the insightful computers envisioned by the field's founders nearly 50 years ago;" *cf.* Michael Slater, *Spam That Almost Passed The Turing Test*, BLACK COFFEE (June 17, 2003), *at* http://karavshin.org/blogs/black-coffee/archive/000426.html (suggesting that spammers and filter builders may be engaged in an arms race, in which it is unclear which side will produce the more-intelligent text-processing robots, based on sophisticated auto-generated e-mail solicitation incorporating multiple quotes from recipient's weblog. The use of weblog quotes attributable to the recipient of the UCE could be anticipated to give "non-spam" indicators when processed through a Bayesian filter whose database is built in part on the weblog author's own legitimate e-mail corpus, which may well include words and phrasing similar to that in his weblog).

that the distribution of such lists effects tortious interference with their business operations.[133] Much of the public undoubtedly has a low opinion of the way UCE promulgators earn a living, and of any alleged constitutional or other justification for mass dispatch of fraudulent spam UCE originators, though, when successfully identified and pursued, have proven more than willing to wrap themselves in the banner of the First Amendment and free trade, and have filed their own actions against anti-spam activists based on a variety of theories.[134]

Still, bolder souls in the anti-spamming community soldier on with proposed direct-action-based solutions such as FFBs ("Filters that Fight Back"). Such programs combine standard filtering functions with "bots" configured to "crawl" to any domain address embedded in a suspected spam, thus potentially overwhelming the spam beneficiary's host domain bandwidth as millions of filters send a query to the domain upon recognizing the suspected spam.[135] Although such tactics arguably skirt close to being an unlawful denial of service ("DoS") attack in their own right,[136] there are more than a few frustrated spam victims in the programming community who seem to have reached the measured conclusion that extremism in the defense of liberty from spam is no vice.[137]

---

133. *See, e.g.*, Jay Hollander, *Anti-Spam Vigilantes and the Law*, GIGALAW.COM (July 2003), *at* http://www.gigalaw.com/articles/2003-all/hollander-2003-07-all.html ("The tort of interference with business involves an effort to drive someone out of business or to harm the business. According to some, that is precisely what anti-spammers are trying to accomplish, without distinguishing between fraudulent spammers and legitimate e-mail marketers."). It is questionable whether a *prima facie* tortuous interference suit against blacklist promulgators could be made out today, to the extent that the blacklist could be shown to contain only domains whose operators had routinely ignored CAN-SPAM's requirements. Early tortious interference allegations were premised on the assumption that UCE was presumptively-lawful commercial speech.

134. *See, e.g.*, Jackie Cohen, *Who's Spamming Whom?*, BEACHBROWSER.COM (1999), *at* http://www.beachbrowser.com/Archives/News-and-Human-Interest/September-99/Whos-Spamming-Whom.htm (recounting AOL's pursuit of notorious UCE entrepreneur Sanford Wallace: "Wallace, like the spammer-defendants who followed, claimed he had a First Amendment right to send spam, and that it was a violation of antitrust laws for AOL to block him from sending spam.").

135. *See* Graham, *Stopping Spam*, *supra* note 127.

136. *Id.*

137. *See, e.g.*, Karl Bode, *Wired Vigilantes: Spam battle gets uglier still*, BROADBAND REPORTS.COM (Aug. 8, 2003), *at* http://www.dslreports.com/shownews/32043 (despairing of any aid being forthcoming from the "utterly flabbergasted and clueless" FTC leadership, and concluding that "[a]s our Spam forum repeatedly indicates, the only thing that seems to really have an impact on spam . . . is vigilantism. Users who are tired of receiving garbage in their inboxes are often hunting the spammer down and doing their best to put them out of business."); Jay Lyman, *Spotlight Forces Exit of New Zealand Spam King*, LINUXINSIDER (Aug. 25, 2003),

The final major approach to technological resolution of the spam problem actually combines technology with economics, seeking to impose infinitesimal delays or costs upon each individual e-mail. Such an approach would – ideally – have a completely unnoticeable effect on any individual or legitimate business e-mail user. But, or so the theory goes, the intentionally-imposed micro-inefficiencies would impose death by a million cuts upon UCE originators, who rely on rapid, and low-incremental-cost, transmission of literally millions of solicitations to maintain a profit margin based upon the minuscule response rate to their solicitations.

So called "slow sender" approaches would require each computer transmitting an e-mail message to perform a somewhat-time-consuming arbitrary calculation before dispatching the e-mail, thus imposing a fraction of a second's delay on each e-mail; irrelevant to individual users, but fatal to spam servers.[138] Unfortunately, such an approach might require adoption of entire new e-mail protocols. If such new protocol adoption were readily-achievable, though, more secure and "spoof proof" versions of SMTP would have emerged years ago as an even more direct solution to the spam problem, instead of remaining a distant promise.[139]

---

at http://www.linuxinsider.com/perl/story/31421.html (conceding, in course of otherwise-disapproving account of harassment of admitted New Zealand spammer Shane Atkinson, who volunteered to stop his activities once his personal contact information was posted on the Internet, that "Atkinson's outing might have been more effective at deterring the 'spam king' than any of the many U.S. legislative efforts to stem the tide of unwanted e-mail."); *see also* Lawrence Lessig, *A Bounty on Spammers*, EWEEK (Sep. 16, 2002), *at* http://www.eweek.com/article2/0,1759,1238770,00.asp (expressing caution regarding current "vigilante" anti-spam efforts, but agreeing that:

> [Spammers] know that attorneys general and ISPs have better things to do than track them down. By making them the only enforcers, spammers know that any law aimed at stopping them will likely not be enforced. . . . If we deputized the tens of thousands of qualified people out there who are able to hunt offenders, then a large number of offenders would be identified and caught.

But see Lester Haines, *US Man threatens anthrax attack on spammers*, THE REGISTER (Nov. 24, 2003), *at* http://www.theregister.co.uk/2003/11/24/us_man_threatens_anthrax_attack/ (outlining possible five year prison term faced by California programmer whose frustration with repeated spam solicitations boiled over into dubious forms of self-help: "Charles Booher, 44, apparently snapped after his computer was deluged with ads offering a larger penis and, presumably not requiring a larger penis at that time, launched a terror campaign against the Canadian company he blamed for the outrage.").

138. *See* Graham, *Stopping Spam*, *supra* note 127.

139. *See id.* (arguing that spammers could likely readily defeat any required time-delaying-calculation, and that "[w]hatever these [slow server] computations were, they couldn't be too arduous, because legitimate corporate mail servers have to be able to send high volumes of mail.").

Another popular proposal for shifting some of the costs of spam back to spammer is the previously-discussed "penny an e-mail" 'postage' proposal, which Microsoft, among others, has championed.[140] However, any Internet postage scheme likely will face great resistance from the independent-minded Internet grassroots and libertarian factions. Moreover, Internet postage schemes have elicited harsh criticism from computer experts as posing "insurmountable" technical problems and threatening serious, but unpredictable, negative effects on the online world.[141]

The keen interest of large companies such as Microsoft in technological solutions to UCE may arise from disinterested concern for its end users' convenience, but seems more likely to be the product of these companies' concern for the millions of dollars that stand to be earned in peddling even partially-effective spam solutions.[142] Indeed, some have even suggested that by treating spam principally as a business opportunity for providing a "killer application" spam solution, major software and Internet companies have contributed to the spam problem (or, as an economic observer of UCE might put it, have done little more than shift the balance of externalities imposed by spam, with little net benefit to its victims).[143]

UCE is a problem having a technical origin, but the financial and social factors[144] contributing to spam's success suggest that no purely-

---

140. *Gates: Buy stamps to send e-mail: Paying for e-mail seen as anti-spam tactic*, (Mar. 5, 2004), *at* http://www.cnn.com/2004/TECH/internet/03/05/spam.charge.ap/ (describing proposals by Microsoft's Bill Gates and companies such as Goodmail for quasi-postage systems as antidote to spam: "At perhaps a penny or less per item, e-mail postage wouldn't significantly dent the pocketbooks of people who send only a few messages a day. Not so for spammers who mail millions at a time.").

141. *See An Overview of E-Postage*, Taughannock Networks (Feb. 2004), *at* http://www.taugh.com/epostage.pdf (citing the massive costs of creating a computer finance and monitoring system robust enough to track and clear payment for the billions of e-mails sent each day; the likelihood of spammer attempts to forge or hijack postage authentication; and consumer distrust of "micropayment" systems as intrinsic flaws in almost all electronic postage schemes).

142. *See, e.g.*, Tim Lemke, *E-mail filters prove big business as spam pours in; Software firms watch revenue soar*, WASHINGTON TIMES (July 17, 2003), *at* http://washingtontimes.com/business/20030716-112006-4134r.htm ("The market to block spam from entering corporate e-mail systems was worth nearly $120 million last year and will grow to $750 million by 2007, according to International Data Corp., a Framingham, Mass., technology-research group.").

143. *See, e.g.*, David Berlind, *Greed: the real reason for Sobig and MyDoom's "success"*, ZDNET (Feb. 2004) ("Were it not for the greed of many e-mail technology companies and [ISPs] who are looking for ways to capitalize on the root cause of [damaging "worms" spread by e-mail] (spam), a majority of the undesirable results from Sobig and MyDoom . . . could have been avoided.").

144. *See, e.g.*, Graham, *Will Filters Kill Spam?*, *supra* note 128:

technological analysis of, or attack upon, spam is likely to yield completely successful results.

E. "Why Bother?"

A fifth way of looking at spam arguably enjoyed a quiet vogue in the United States, at least in official circles, for many years. Some officials and commentators still seem to embrace this view: namely, that spam is an inevitable and insoluble (but manageable) fact of online life. The FTC's failure, over many years, to adopt a role much more active than that of spam museum curator seems to support the notion that the analytical framework chosen for analyzing UCE has significant effects on the action (if any) that the analyzing party will adopt, or even contemplate as feasible, for fixing it.

Of course, the FTC was not alone in viewing UCE problems as beyond the realm of any practical solution. Congress's long-delayed efforts at enacting a federal anti-spam statute (*see supra* Section II) veered between ineffectual paroxysms of alarm at the menace of spam, and overly-blithe assurances that often-simplistic statutory provisions would be sufficient to annihilate UCE abuse.

One variant of the "no solution to spam" worldview is that the Internet is inherently unsecurable, and thus there will always be significant gaps in any technological protection scheme.[145] Notably, this view is not inconsistent with adopting portions of the technological-solutions oriented analysis of spam. Indeed, the same person may simultaneously be pessimistic about the ability of technology ever effectively to eliminate UCE abuse, while still adopting certain technological countermeasures that he finds partially effective.[146]

> The person who responds to spam is a rare bird. Response rates can be as low as 15 per million. That's the whole problem: spammers waste the time of a million people just to reach the 15 stupidest or most perverted.
>
> If we want to make spam stop working, we have to somehow prevent the 15 idiots from responding to the spams that are sent to them. Otherwise the spammers will keep sending it to everyone. So, strangely enough, whether or not filtering will kill spam depends entirely on what those 15 idiots do.

145. *See Fighting a Losing Battle Against Spam*, DEUTSCHE WELLE (Mar. 16, 2003), *at* http://www.dw-world.de/english/0,3367,1446_A_809287,00.html; Lee Ann Roman, *Solutions for deleting pesky spam problem are slippery*, BIZWOMEN.COM (Nov. 14, 2003), *at* http://www.bizjournals.com/memphis/stories/2003/11/17/focus4.html ("[C]ombating spam will be a continual investment for businesses because solutions must change to meet the problem, technology managers say.").

146. *See, e.g.*, *Anti Spam Fanatics*, *at* http://www.mailmsg.com/SPAM_anti_spam_fanatics.htm (bemoaning fact that "there is no solution for spam. Period. Nothing works well, no solution is perfect, and due to the design of internet email, nothing can ever work well.

Another variant of this analysis often does not reach the issue of whether regulation of, or high-tech countermeasures against, UCE are feasible, because this variant approach regards any threat posed by UCE as minimal and not worth taking the time to complain about, or waste government or technologists' time on.[147] This "just press delete" school of thought may never have been very widespread beyond the ranks of self-interested marketers trying to soothe enraged spam recipients. But if disinterested parties ever believed that simply ignoring or deleting unwanted UCE was an option, it seems doubtful whether they would remain as sanguine today, when the volume of spam and the pernicious tactics used to disseminate it have expanded many-fold.[148]

A final species of the "spam is insoluble" mindset arose from the belief that no legal remedies were practically available against UCE abuse. Some argued, for instance, that enacting state or national anti-spam laws was pointless because most spam originated from, or could be moved to, offshore domains beyond the territorial reach of such laws.[149] We have discussed at length (and will further mention in

---

At least, not without some serious changes to the basic design of email," but also describing author's implementation of filtering and other counter-measures as partial remedies that decreased incoming spam on his computer).

147. *See, e.g.*, Barry Dennis, *Why I love spam*, CNET NEWS (May 16, 2002), *at* http://news.com.com/2010-1071-915523.html ("There are some e-mails I get that I don't want or appreciate: pornography, two credit card offers every day . . . and some others. But you know what I do? Hit delete. I hit delete, and I'm free."); *Online Marketers Say So-Called Spam Threat Is Overblown*, INTERNETWEEK.COM (June 27, 2003), *at* http://www.internetweek.com/story/showArticle.jhtml?articleID=10809956 (quoting electronic marketing businessman: "Really, there are more important things in life [than spam regulation] . . . . Nobody likes spam, junk mail, commercials, billboards, telephone solicitors and of course door-to-door salespeople. . . .But hey, everything comes with a price, including freedom.").

148. Press Release, *Eliminating Spam Requires Team Effort: New Technology and Precautions by Computer Users Take Biggest Bite Out of Spam*, MICROSOFT (Mar. 11, 2004) (continuing Microsoft's longstanding advice to "just delete" spam, but also recommending use of filters and e-mail address concealment).

149. *See, e.g.*, *California spammers to move offshore*, VIGILANT.TV (Oct. 4, 2002), *at* http://vigilant.tv/article/2294 (citing California's spam regulation efforts as "a neat example of why anti-spam laws can't possibly work . . . . even if they're successful [in identifying California-based UCE], spammers will simply move offshore."); Phil Raymond, *Will the vendetta against spam kill e-mail as we know it?*, SEARCHSECURITY.COM (June 30, 2003), *at* http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci912603,00.html ("In fact, most spam originates from outside the United States in the Baltic and far-east . . . .The ability for any government to trace and prosecute a sender for harassing individual recipients is impractical and futile in its potential for prosecution."); *but see* Press Release, *Sophos outs 'dirty dozen' spam producing countries*, (Feb. 26, 2004), *at* http://www.sophos.com/spaminfo/articles/dirtydozen.html ("'The United States is far and away the worst offender, accounting for nearly 60 percent of the world's spam . . . .'"); *Debunking Offshore Spam*, TAINT.ORG, *at* http://taint.org/2003/11/24/191116a.html (ranking U.S. as chief source of spam originators and

Subsection (F) *infra*) the challenges to legislative or regulatory attempts to define and regulate UCE or spam. However, the most fundamental form of the "no legal remedy" school of thought did not merely point to practical challenges in implementing anti-spam laws. Instead, it effectively denied that spam was subject to legal redress in the first place.

Many a rueful commentator shook his head before the effective date of the CAN-SPAM Act, citing as the central problem in any spam regulation attempt the "fact" that "spam is not illegal."[150] This was certainly the view taken by most of the government, most of the time.[151] Given what we now know, and what the government could have then known, regarding the disproportionately-fraudulent nature of most UCE return address and header information, not to mention the often-illegal nature of the goods and services being touted by spam,[152] and the racketeer-like organization and conspiring of spam gangs,[153] it should not have taxed the imagination of a regulator[154] or prosecutor as much as it apparently did in many cases to develop grounds for criminal or civil action against UCE abusers, notwithstanding the absence of a specific anti-spam statute.[155] Several spammers were subjected to criminal and civil penalties for

---

beneficiaries, though U.S. based spammers may mask this fact by using hijacked foreign relay computers; and arguing that even if majority of spammers were offshore operators, "'that fact does not negate the need for or effectiveness of laws against those in the US. It can be very difficult to bring a murderer to justice in the US if they escape abroad, but no one could seriously argue that this fact means domestic murder laws are unnecessary or irrelevant.'" (citation omitted)).

150. *See, e.g.*, Fred Grimm, *Bogus Boca: The Spa for Spam*, MIAMI HERALD (May 29, 2003), *at* www.miami.com/mld/miamiherald/news/columnists/fred_grimm/5964205.htm (describing career of accused arch-spammer and convicted criminal Eddy Marin, but noting that "spam is not illegal.").

151. *See, e.g.*, James Gleick, *Tangled Up In Spam*, NY TIMES (Feb. 3, 2003), *at* http://www.noblit.com/docs/Tangled-Up-In-Spam.pdf (noting as of 2003 that FTC repository for spam was receiving about 85,000 alleged spasm daily, and that "[e]very month or so, the commission files an enforcement action against someone, leading to a warning letter, or a promise by the spammer to cease and desist... The agency can't help noticing that, by and large, spam is not illegal.").

152. *See supra* notes 8, 109 and accompanying text.

153. *See* Gleick, *supra* note 151.

154. *Id.* (quoting FTC staff lawyer explaining that the agency cannot pursue most spammers, only those involved in "deceptive" conduct, then allowing in response to reporter's inquiry that "Maybe there's a deceptive statement about how your name was acquired" in false representations that UCE is being sent to consumers based on previous (and non-existent) opt-in or "subscription").

155. *See, e.g.*, Doug Isenberg, *Despite Outcry, Existing Laws Already Restrict Spam*, GIGALAW.COM (Sept. 2000), *at* http://www.gigalaw.com/articles/2000-all/isenberg-2000-09a-all.html.

pre-CAN-SPAM Act conduct.[156] These successful investigations and prosecutions indicate that even without a spam-specific federal law, spammers were not immune from the tender attentions of vigorous and imaginative police and prosecutors.[157] Conversely, some in law enforcement positions acted (and perhaps continue to act) less effectively against spam than they might otherwise have done, due to an apparent inability to envision the problem in any light other than that of the long-stalled federal spam prohibition, despite clear evidence of UCE abuses that constituted violations of many already-existing legal prohibitions.

F. "The Legal System Is Working . . . Sort Of"

No one who deals with an e-mail account on a daily basis would be rash enough to suggest that the current legal regime has abolished the spam problem. But some do view the spam problem as fundamentally amenable to significant amelioration through legal mechanisms.[158]

Believing that laws are among the proper tools to deploy against UCE abuse does not answer two crucial subsidiary questions: which laws can be effective against spam, and how effective need they be?

---

156. *See supra* Section IV(c); *see also* Saul Hansell, *Virginia Indicts 2 Under Antispam Law*, NY TIMES at C4 (Dec. 12, 2003) (announcing indictments under Virginia's unsolicited bulk e-mail criminal statute); Paul Roberts, *'Buffalo Spammer' convicted*, COMPUTERWORLD (Apr. 1, 2004), *at* http://www.computerworld.com/securitytopics/security/cybercrime/story/0,10801,91823,00.html?SKC=security-91823 (detailing conviction of notorious 'Buffalo Spammer' on charges of identity theft and falsifying business records in connection with his setting up of multiple e-mail accounts in other parties' identities for purpose of concealing UCE activity).

157. The demonstrably-fraudulent nature of much UCE also largely obviates the oft-voiced pessimism that stringent anti-spam legislation would face significant constitutional hurdles, under even the diluted protections afforded to commercial speech, given the prerequisite that such commercial speech not be deceptive or unlawful in nature.

158. *See, e.g.*, Graham, *supra* note 127 (endorsing anti-spam laws in concept, although warning that careful drafting to avoid loopholes, and strong enforcement, will be necessary to achieve such laws' potential to "eliminate 80% of spam, if done right."); Dennis McCafferty, *Can CAN-SPAM Really Stop Spammers?*, WEB HOSTING MONTHLY (Jan. 2004), *at* http://thewhir.com/features/can-spam.cfm (quoting e-mail performance management expert Matt Blumberg: "Will [CAN-SPAM] have a positive impact in the war on spam? Absolutely. . . .[T]his legislation should help lessen spam by giving the federal government the authority it needs to hand out fines and jail time to offenders; by setting clear minimum standards for legitimate mailers to follow; and, perhaps most useful of all, by providing a way for the average consumer to identify and report spam.").

Beyond its sponsors,[159] no one seems to believe that CAN-SPAM alone, at least as currently implemented, will have much noticeable effect in curbing spam. With a few anomalous exceptions,[160] spam volumes do not seem to be decreasing at all in the months since the Act went into force, but are instead increasing.[161] Nonetheless, ISPs and others affected by spam continue to devote considerable resources to litigation under both the Act[162] and other legal theories.[163] These efforts indicate that companies and individuals continue to believe that anti-spam laws, individually or in combination, can provide meaningful redress justifying the expensive, and often frustrating, task of chasing UCE promulgators to ground. AOL's recent, and highly-publicized, contest giving away a Porsche seized in satisfaction of a pre-CAN-SPAM civil judgment against a spammer sent a clear signal that corporations affected by spam would seek to punish alleged spammers by attacking their most treasured assets, through a variety of avenues, so as to reduce the perceived financial incentives to set up shop as a UCE distributor.[164]

But how much litigation and regulatory success is enough to stem the tide of spam? If it is true that spammers can profit with

159. Amit Asaravala, *With This Law, You* Can *Spam*, WIRED (Jan. 23, 2004), *at* http://www.wired.com/news/business/0,1367,62020,00.html (quoting, skeptically, spokesman for Act sponsor Sen. Ron Wyden as arguing that CAN-SPAM, despite pre-empting state anti-spam statutes, will empower states to fight spam more effectively because of its authorizations of civil actions by state attorneys general).

160. *See* Janis Mara, *AOL Reports Drops in Both E-Mail and Spam Volume*, CLICKZNEWS (Mar. 19, 2004), *at* http://www.clickz.com/news/article.php/3328841 (reporting 37% drop in incoming AOL messages identified as spam during early months of 2004).

161. *See supra* notes 74.

162. *See* Kris Oser, *Big ISPs File Suits Under Can Spam*, DIRECT NEWSLINE (Mar. 10, 2004), *at* http://www.directmag.com/ar/marketing_big_isps_file/ (reporting filing of six lawsuits against hundreds of named and John Doe defendants by ISPs AOL, Earthlink, Microsoft, and Yahoo for a variety of alleged violations of the Act in connection with millions of solicitations sent to the ISPs domains. The DMA cooperated with and supported the ISPs in their lawsuit filing, and Act co-sponsor Sen. Conrad Burns used the occasion to laud CAN-SPAM as "empower[ing] Internet users as they navigate the Net.").

163. *See, e.g.*, Brian McWilliams, *No Truce in the Spam Wars*, WIRED (Sept. 10, 2003), *at* http://www.wired.com/news/business/0,1367,60357,00.html (reporting on crusading anti-spam lawyer Pete Wellborn's campaign against Boca Raton-based alleged spammers, in which he sought attorneys fees and threatened to follow up on previous multi-million dollar verdicts against spammers, based on allegedly-frivolous litigation brought by UCE front-group EMarketers America.org seeking to curtail anti-spam activism).

164. *Spammer's Porsche up for grabs*, BBC NEWS (Mar. 30, 2004), *at* http://news.bbc.co.uk/1/hi/business/3581435.stm (detailing raffle of $47,000 sports car seized from unidentified spammer who made over one million dollars by sending one billion e-mails flogging pornography, college diplomas, illegal cable descramblers, and other products to AOL members).

response rates of fifteen out of one million, it seems that only a law (or combination of laws) significantly more stringent than CAN-SPAM could, standing alone, provide sufficient disincentive to spammers to induce them to eschew the still-relatively-small risks they incur in sending out their anonymous missives. Of course, this calculus could be changed if technological or standards-based developments significantly diminished the ease with which spammers can currently hide the source of UCE.

Other deficiencies in our factual knowledge of the true nature of the spam epidemic may also make it difficult, even for those committed to a civil and criminal law-enforcement approach to battling UCE, to assess realistically the odds of success from such an approach. For instance, the commonly-encountered anecdotal statement that a small number of hugely-prolific U.S.-based spam gangs account for a substantial majority of spam[165] would – if true – lend greater credence to the view that a coordinated U.S. law enforcement approach could ultimately remove a substantial proportion of spam from the e-mail stream. Conversely, if the sources of spam are significantly more diffuse than the anecdotal figure suggests, legal action against individual spammers could appear much less promising. It would be comforting to think that the FTC, in its decade-long, placid contemplation of the contents of its spam museum, had been making meaningful qualitative and quantitative evaluations of such strategically-crucial characteristics of the UCE marketplace. More realistically, further study of such practical factors may be necessary before it is possible to come to useful conclusions as to the magnitude of the role that existing, revised, or new civil and criminal provisions can play in effectively reducing spam.

CONCLUSION

The CAN-SPAM Act will almost certainly prove insufficient, by itself, to thwart the explosion of spam. CAN-SPAM emerged during

165. *See, e.g.*, Robert Bruce Thompson, DAYNOTES JOURNAL (Aug. 28, 2003), *at* http://www.ttgnet.com/daynotes/2003/2003-35.html (asserting that "[t]he overwhelming majority of spam messages are produced by just a few major spammers. I've seen various estimates, but certainly the top 200 spammers are responsible for at least 80% and probably 95% of the spam generated world-wide," but suggesting the effective response to this fact would consist not so much of a litigation-based campaign against these spam kingpins, but rather would involve a program of selective assassinations of exemplary identified spammers: "Imagine the effect if tomorrow morning CNN reported that a major spammer had been found shot to death, with a 'No Spam' postcard pinned to his chest.").

an era in which industry observers and policy makers have viewed the UCE problem in markedly different ways by employing divergent analytical frameworks regarding the nature of e-mail and UCE, and have accordingly proposed an array of diverse, not-wholly-consistent, solutions influenced by these differing analytical approaches. None of these solutions appears free from shortcomings, just as CAN-SPAM will likely be hobbled in part by flawed, naive, or politically-influenced analyses or curative approaches embraced during the start-and-stop process that finally yielded the Act as the unimpressive product of years of legislative dithering.

A successful hybrid approach to combating spam will likely involve significant embrace of the economic and technological analyses of spam, to identify and address the imbalances or inefficiencies in the e-mail market that make spam feasible and lucrative, and to provide technological defenses based on the assumption that there will always remain an economic incentive for some persons to abuse Internet-based communications. Development of effective economic- and technology-based spam remedies will depend in part on understanding more than we currently know about the exact nature, extent, motivations for, and source of spam, and about specific methods that have, or have not, yielded tangible success in neutralizing it.

The need for economic and technical measures against spam does not imply that law-based analyses and remedies cannot play an important and effective role against UCE. CAN-SPAM was neither the first, nor should it be the last, weapon in the legal arsenal against UCE abuse. It may yet play a demonstrably-useful role, in conjunction with pre-existing common law and statutory doctrines, in making spammers pay financially and penally, and thus in reducing the so-far accurate perception that spamming truly has no incremental cost, fiscal or otherwise, for its perpetrators. In this connection, Congress should likely consider amendments to CAN-SPAM, whether to remove the strict pre-emption provision[166] that limits state attempts to address spam, or to impose more stringent remedies, such as an opt-in approach or private rights of action, to increase consumer options against spam and put spammers on the defensive. Effective international cooperation in the legal war against spam will be

166. *But see* S. 877, *supra* note 1 at § 8(b)(1)–(2) (preserving from pre-emption certain state anti-fraud and consumer protection legislation, even as applied to e-mail); *see also supra* note 61 (discussing the possibility that state laws falling within Act's non-preempted safe harbor may continue to play a role in fighting spam).

important,[167] and should not be unattainable, given that national governments are among those on whom spammers currently impose their economic externalities.

Taking on the world's UCE bandits will not be an easy task, and will require clearer thinking, better coordination, and more resoluteness of purpose, than manifest themselves in the history and application to date of CAN-SPAM and other United States legal approaches to spam control.

167. *See, e.g.*, Gilbert Le Gras, *Canada Eyes World Treaty to Deal with Spammers*, REUTERS (May 11, 2004), *at* http://www.reuters.com/newsArticle.jhtml (noting proposals by Canadian head of Organization of Economic Cooperation and Development working party on information security and privacy for international treaty, and perhaps extradition provisions for suspected spam kingpins, to address perceived shortcomings in existing national anti-spam laws).